UNIVERSITIES SOUTH AFRICA

POPIA INDUSTRY CODE OF CONDUCT: PUBLIC UNIVERSITIES

TABLE OF CONTENTS

A. INTRODUCTION

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. USAf has decided to draft a Code of Conduct to help regulate the processing of personal information within the Higher Education Industry to comply with the POPIA.

The Protection of Personal Information Act (POPIA) was approved on 19 November 2013 to protect the personal information processed by public and private bodies. On 22 June 2020 new effective dates were announced for certain sections of the Protection of Personal Information Act[1] (the 'POPIA').[2] From 1 July 2020 sections 2 to 28, 55 to 109, section 111, and section 114(1) – (3) will be in force. From 30 June 2021 Section 110 and section 114(4) will be in force. Organisations which process personal information are being given one year from these dates to become fully compliant with these sections of the POPIA. This means that South African Universities must comply with POPIA by 30 June 2021.

2. PURPOSE OF THE CODE

This Code is intended to take the principles set out in the POPIA and apply these principles to the Industry in a way that empowers the Industry and clarifies the requirements of the POPIA. The purpose of the Code is to:

- increase the level of the protection of privacy within the Industry by aligning the Industry's approach to information governance specifically privacy, with that of the Information Regulator;

- ensure the uniform and industry-appropriate implementation of the POPIA by helping public universities comply with the POPIA and promoting good information and technology governance to achieve the institution's strategic objectives[3]; and

[1] The Protection of Personal Information Act 4 of 2013.
[2] Commencement of certain sections of the Protection of Personal Information Act, Proclamation No. R.21 of 2020, Government Gazette 43461, 22 June 2020.
[3] Principle 12 of the King IV Report on Corporate Governance in South Africa.

- provide for the responsible use of personal information within the Industry.

3. STATUS OF THE CODE

3.1. The current status of the Code

In terms of the POPIA the Information Regulator may accredit a code of conduct for a specific industry, and although this Code has not been accredited by the Information Regulator in terms of the POPIA, it has been drafted with the intention of being accredited. However, until then, the adoption of the Code is voluntary.

The Code has been adopted as a guideline by the Board of Universities South Africa. Guidelines are different from rules in that they are not absolute; they indicate what public universities should do, not what they must do.

As the POPIA is based on a reasonableness standard, departures from what is considered best practice under the circumstances are allowed, but all decisions must be motivated.

3.2. The status of the Code once it is accredited

Once this Code has been accredited a failure to comply with it will be considered a breach of the conditions for lawful processing under the POPIA.[4]

When will an application for accreditation be made?

Applications for the accreditation of Codes of Conduct are governed by Chapter 7 of the POPIA. This Chapter will become effective on 30 June 2021. Once Chapter 7 is effective an application for accreditation will be submitted.

4. SCOPE OF THE CODE

This Code applies to all processing of personal information by 'public higher education institutions' as defined in section 1 of the Higher Education Act, 101 of 1997.

The following definitions in the POPIA are key in determining what activities undertaken by public higher education institutions will be affected by the Code:

Personal information	'Personal information' means information relating to an identifiable, living, natural person, and where it is 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,

[4] Section 68 of the Protection of Personal Information Act, 4 of 2013. The definition of 'this Act' in section 1 includes all regulations and codes of conduct.

	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.
Special personal information	'Special personal information' means (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.[5]
Data subject	'Data subject' means the person to whom personal information relates. Data subjects may include: • prospective students • student applicants • South African and international students

[5] The definition of 'special personal information' in section 1 read with section 26.

	• exchange students • post-doctoral fellows • alumni • academic and administrative staff • employment candidates • external members of committees • employees • researchers • research participants • authors • council members • service providers, suppliers, independent contractors • partner organisations • subsidiaries • donors and funders • visitors • members of the public
Processing	'Processing' means 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.

5. INTERACTION WITH EXISTING LEGISLATION, CODES, AND GUIDELINES

The POPIA is not the only piece of legislation that affects the processing of personal information in the Industry. Here are other examples of such legislation:

- The Constitution of South Africa[6]
- the Higher Education Act[7]
- Regulations for reporting by Public Higher Education Institutions (2014)[8]
- the National Qualifications Framework Act[9]
- the Continuing Education and Training Act[10]
- the Skills Development Act[11]
- the National Health Act[12]
- Ethics in Health Research Guidelines[13]
- the Consumer Protection Act[14]
- the National Credit Act[15]
- the Close Corporations Act[16]
- the Compensation for Occupational Injuries and Diseases Act[17]
- the Copyright Act[18]
- the Promotion of Access to Information Act[19]
- the Electronic Communications Act[20]
- the Electronic Communication and Transaction Act[21]

[6] The Constitution of the Republic of South Africa, 1996.
[7] No 101 of 1997.
[8] No 101 of 1997.
[9] No 67 of 2008.
[10] No 16 of 2006.
[11] No 97 of 1998.
[12] No 61 of 2003.
[13] Ethics in Health Research Guidelines, 2015.
[14] No 68 of 2008.
[15] No 34 of 2005.
[16] No 69 of 1984.
[17] No 130 of 1993.
[18] No 98 of 1978.
[19] No 2 of 2000.
[20] No 25 of 2002.
[21] No 25 of 2002.

- the Employment Equity Act[22]
- the Labour Relations Act[23]
- the Income Tax Act[24]
- the Intellectual Property Rights from Publicly Finances Research and Development Act[25]
- the Basic Conditions of Employment Act[26]
- the Broad Based Black Economic Empowerment Act[27]
- the National Archives and Records Services of South Africa[28]
- the Promotion of Administrative Justice Act[29]
- the King Codes of Corporate Governance

Relevant section:

Section 3(2) (Application and interpretation of the Act)

When there is a material inconsistency between the POPIA and other legislation, the POPIA will apply.[30] Conversely, if the other legislation provides more extensive protection than the POPIA, the other legislation will apply.[31] For example:

- If other legislation requires that personal information must be processed (such as the National Credit Act[32] which requires that certain personal information must be collected), Universities must comply with it in addition to the POPIA.
- If other legislation contains a provision which mandates that a particular type of personal information (e.g. employment records) must be kept for a specific period, that legislation will still apply. The University must still comply with the rest of POPIA.
- If other legislation is silent on the processing of personal information, the POPIA will apply.

[22] No 55 of 1998.
[23] No 66 of 1995.
[24] No 58 of 1962.
[25] No 51 of 2008.
[26] No 75 of 1997.
[27] No 53 of 2003.
[28] No 43 of 1996.
[29] No 3 of 2000.
[30] Section 3(2)*(b)* of the POPIA.
[31] Section 3(2)*(c)* of the POPIA.
[32] No 34 of 2005.

- If other legislation provides more extensive protections (e.g. the Constitution provides that no person can be forced to participate in scientific research without their consent), the more extensive protections must be provided.

B. APPLICATION OF THE POPIA

1. THE DEFINITION THAT DETERMINES THE APPLICATION OF THE POPIA

The following questions can be used to establish whether the POPIA applies:

- 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 the personal information in South Africa?

Relevant section:

Section 3 (Application and interpretation of Act)

1.1. Is the institution 'processing' 'personal information'?

The definitions of 'processing' and 'personal information' are extensive.

1.1.1. What is 'processing'?

Relevant section:

The definition of 'processing' in section 1

'Processing' includes any activity relating to personal information. The definition of processing describes the entire life cycle of personal information, namely:

- collecting or creating personal information;
- utilising personal information;
- storing personal information;
- sharing personal information; and
- retaining, or destroying personal information.

The POPIA prescribes rules for each phase in the information life cycle. The POPIA applies regardless of how the processing is done (i.e. whether it is 'automated' or not), as long as personal information is entered into a 'record' and forms part of or is intended to form part of a 'filing system'. The definitions of 'record', 'automated' and 'filing system' are discussed in section 1.2 below.

1.1.2. What is identifiable 'personal information'

Relevant section:

The definitions of 'personal information' and 'data subject' in section 1

The definition of 'personal information' extends the POPIA's application to all information that can be linked to an identifiable living individual, or existing juristic person.

The individual or juristic person to whom the personal information relates is referred to as the 'data subject'. While the POPIA's definition of 'personal information' expressly refers to living individuals, the Promotion of Access to Information[33] does not which explains why PAIA requests will continue to include requests for access to records relating to deceased persons.[34]

The POPIA does not apply when personal information cannot be linked to an identifiable individual or company.

Thus, if the link between the information and the data subject can be severed, a process referred to as de-identification or anonymisation, the POPIA no longer applies. De-identification or anonymisation is often done when an institution wants to publish or disclose information, for instance, with the publication of research.

Relevant section:

The definitions of de-identify in section 1

Information is considered de-identified if the information cannot be re-identified by any reasonably foreseeable method or through linking it with other information that identifies the data subject. This distinguishes de-identification from masking or pseudonymisation.

What is pseudonymisation?

Information is pseudonymised when the identifying fields are replaced by pseudonyms and the information cannot be linked to a specific data subject without additional information. Pseudonymisation is a very effective technique for securing information as a person needs both the record of personal information as well as the additional information in order to link the personal information to a specific data subject.

It is considered best practice to pseudonymise personal information whenever it is appropriate. Pseudonymisation is an important example of 'data protection by design'.[35]

Information is considered to be de-identified, if:

- the data subject cannot be identified directly or indirectly from the personal information itself; or

[33] No 2 of 2000.
[34] Access requests are discussed in part C, section 17.1.
[35] See article 25(1) of the GDPR.

- it is not possible to re-identify the information by linking it to other information (e.g. public information, information held by another institution, or the government). If re-identification is possible, but unlikely, this risk must be measured and documented before a decision is made on whether the level of anonymisation is adequate.

Institutions should:[36]

- have policies and processes in place to authorise, oversee, and assess all anonymisation processes;
- ensure that personal information is de-identified if there is no purpose for which the identity of the data subject is relevant[37]; and
- consider whether pseudonymising is practical before commencing processing activities.

1.2. Is the 'personal information' entered into a 'record' and does it form part of a filing system?

Relevant section:

- The definition of 'automated means' in section 3(4)
- The definition of 'filing system' in section 1
- The definition of 'record' in section 1

For the POPIA to apply, the personal information must be entered into a record. In terms of section 3(1):

- The personal information must be entered into a 'record' for or by the responsible party. A 'record' includes any form or medium. Examples include writing on any material, digital or computerised record, books, graphs, photographs, films, and tape recordings. How to determine who the responsible party is, is discussed in part C, section 1, but it should be noted that all public universities will be the responsible parties in respect of many processing activities.
- The personal information can be entered into a record by 'automated or non-automated means. 'Automated means' is defined in section 3(4) and in essence, refers to processing done by computer.

36 See the International Association of Privacy Practitioner's Guide to *Basic Data Anonymization Techniques*.
37 Consent is not required to de-identify information. This is largely based on commentary to the EU GDPR that de-identification is considered compatible with the original purpose of processing as long as the de-identification process reliably produces fully and permanently de-identified information. Article 29 Data Protection Working Party Opinion 5/2014 on Anonymisation Techniques 7.

- If non-automated means are used, the personal information must also form part, or be intended to form part of a 'filing system'. 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 definition can include 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 can handle complex search queries.

1.3. Is the 'responsible party' domiciled or is processing taking place in South Africa?

For the POPIA to apply:

- the responsible party must be domiciled in South Africa; or
- the responsible party must use automated or non-automated means to process the personal information in South Africa.

Because all public universities of South Africa are domiciled in South Africa the POPIA would apply to them.

The POPIA may also apply to institutions that are domiciled elsewhere if an institution in South Africa is processing personal information on behalf of those institutions, regardless of whether the processing is automated or non-automated.

2. THE POPIA WILL APPLY TO ALL PUBLIC UNIVERSITIES

All South African public universities process personal information of, amongst others, the following data subjects:

- prospective students
- student applicants
- South African and international students
- exchange students
- post-doctoral fellows
- alumni
- academic and administrative staff
- employment candidates
- external members of committees
- employees

- researchers
- research participants
- authors
- council members
- service providers, suppliers, independent contractors
- partner organisations
- subsidiaries
- donors and funders
- visitors
- members of the public

This means that the POPIA will apply to all public universities of South Africa.

C. THE PRINCIPLES OF LAWFUL PROCESSING OF PERSONAL INFORMATION

Part C contains general principles and standards that apply to all personal information processing activities.

1. ESTABLISH WHO IS RESPONSIBLE FOR COMPLIANCE

Relevant section:

- Section 8 (Responsible party to ensure conditions for lawful processing)
- The definition of 'responsible party' in section 1
- The definition of 'operator' in section 1

The responsible party is the institution that has control over why and how personal information is processed, including decisions such as:

- to collect the personal information and whether there is a legal basis for the collection;
- 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 and to whom;
- whether to give data subjects access to their personal information;
- how long to keep the personal information; or
- whether to make non-routine amendments to the personal information.[38]

Other institutions that process the personal information, but who are not responsible parties, are operators. Operators may make some decisions about how to process the personal information on behalf of the responsible party.

[38] Information Commissioner's Office *Data controllers and data processors: what the difference is and what the governance implications are* (2014) from 6. The definitions of 'responsible party' in terms of the POPIA and the definition of 'controller' in the GDPR are very similar. This means that it is appropriate to take guidance from the work of European regulators.

This includes decisions about:

- what systems to use;
- how to store the personal information;
- what security measures to put in place;
- how to share the personal information; or
- how to delete personal information.[39]

When institutions process personal information together, they must:

- ensure that there is no confusion about their respective roles and responsibilities for POPIA compliance;
- establish their roles and responsibilities before processing starts; and
- document their roles and responsibilities in a written agreement between them.

The sharing of personal information between responsible parties and operators is discussed in part C, section 16.

2. THE PURPOSE FOR PROCESSING MUST BE SPECIFIC, EXPLICITELY DEFINED, AND DOCUMENTED

Relevant section:

- Section 13(1) (Collection for specific purpose)
- Section 17 (Documentation)

Personal information must be collected for a specific, explicitly defined, and lawful purpose. To comply with this requirement institutions should:

- create an inventory of all of the personal information it has; and
- determine the purposes for which the personal information was collected.

[39] Information Commissioner's Office *Data controllers and data processors: what the difference is and what the governance implications are* (2014) from 6. The definitions of 'operator' in terms of the POPIA and the definition of 'processor' in the GDPR are virtually identical. This means that it is appropriate to take guidance from the work of European regulators.

Specifying the purpose for which personal information was collected is a prerequisite for complying with many other requirements. The following are examples of problems that are created when the purpose for collection is not well defined:

- It may be impossible to establish who the responsible party is. This is discussed in part C, section 1.
- The lawfulness of a particular processing activity cannot be assessed without knowing what the purpose of the processing is. This is discussed in in part C, section 2.
- It is difficult to assess the quality of the personal information as institutions do this in relation to the purpose for collecting. This is discussed in part C, section 12.
- The transparency requirements cannot be met. This is discussed in part C, section 9.
- Personal information cannot be deleted when it is no longer needed if the purpose for collecting the information is not known. This is discussed in part C, section 14.

The purpose for collecting personal information must be specific and explicitly defined. This means that it must be 'stated clearly and in detail, leaving no room for confusion or doubt'.[40] Institutions must document the purposes for which personal information is processed[41] before any personal information is collected and processed.[42]

3. THERE MUST BE A LEGAL BASIS FOR PROCESSING

Relevant section:

Section 11(1) (Justification)

Once the purpose for processing the personal information has been determined, the lawfulness of the processing activity must be assessed. All processing activities must have a legal basis. The POPIA refers to this as 'justification' and it provides several justifications for processing activities.

Before institutions collect and process any personal information, they should document:[43]

- the justification for processing they are relying on; and
- their reason for relying on that justification.

Each of the justifications listed in section 11(1) is discussed here.

[40] English Oxford Living Dictionaries *'Explicitly'* accessed at https://en.oxforddictionaries.com/definition/explicitly, last accessed on 22 August 2018.
[41] Section 13(1).
[42] Given that the POPIA is new, most institution will have to take this step *ex post facto*.
[43] Given that the POPIA is new, most institutions will have to take this step *ex post facto*. This requirement will apply to all new processing activities.

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

3.1.1. The scope of this justification

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

There are two potential grounds on which processing will be justified. The processing is 'necessary to carry out actions for the' conclusion or the performance of the contract.

Here the word 'necessary' must be interpreted narrowly. Whether the particular processing activity is necessary must be measured against the exact reason for the contract, i.e., the 'substance and fundamental objective' of the contract.[44] Mentioning the particular processing activity in the contract will not be enough.[45]

Example: Student applications

When students apply to university they are asked for personal information in order 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 personal information to do a means test. These processing activities are clearly necessary for the conclusion of the contracts. 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 will have to 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 for the conclusion and performance of the employment contract. For instance, the processing of bank account details to pay salaries. However, this will not be the case for all processing activities. For instance, 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 employer should rely on the justification that it is in its legitimate interest to monitor employees.

3.1.2. When this justification does not apply

[44] Article 29 Data Protection Working Party *Opinion 6/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* 17. The guidance was issued under the 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 ('the Data Protection Directive'). There are no plans to issue a new guidance, but this version is still in use (Information Commissioner's Office *GDPR Guide* 86). Section 11(1)*(b)* is very similar to article 6(1)*(b)* of the GDPR and article 7*(b)* of the Data Protection Directive. This means that it is appropriate to take guidance from the official guidelines issued by the Article 29 Data Protection Working Party.

[45] Article 29 Data Protection Working Party *Legitimate Interests* 16.

This justification cannot be relied on to process special personal information.[46] Justifying the processing of special personal information is discussed in part C, section 4.

3.2. Personal information may be processed to comply with an obligation imposed by law

3.2.1. The scope of this justification

If the law requires that a particular processing activity must take place, the processing is justified. For instance, where legislation authorises the collection of personal information by the Government.[47]

Example: Complying with reporting requirements

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

Example: Labour legislation

The Employment Equity Act[48], the Labour Relations Act, and the Basic Conditions of Employment Act provide justification for the processing of large amounts of employee information.

The legal provision itself must also be POPIA compliant. For instance, the processing must be necessary to fulfil the purpose of the legal provision and it must be the least invasive way to achieve that purpose. The POPIA states that it will apply 'to the exclusion of any other legislation that regulates the processing of personal information and that is materially inconsistent with an object, or specific provision' of the POPIA.[49]

What if there are contradictory legislative requirements?

Refer any contradictory legislative requirements to USAf who will refer the matter to the Information Regulator for clarification.

Sharing information with other institutions (including the government) is discussed in detail in part C, section 16.

3.2.2. When this justification does not apply

This justification does not apply if the institution has a choice whether to comply with the obligation. For instance, voluntary collaboration with public authorities are not covered by this justification.[50]

[46] The justification is not listed in section 27(1).
[47] The sharing of information with the Government is discussed in part C, section 16.
[48] 55 of 1998.
[49] Section 3(2)*(a)*. Also see Article 29 Data Protection Working Party *Legitimate Interests* 19.
[50] Article 29 Data Protection Working Party *Legitimate Interests* 19.

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

3.3.1. The scope of this justification

The processing of personal information will be justified if the processing activity protects a legitimate interest of the data subject.[51] 'Legitimate interest' in this context often refers to the health and safety of the data subject.[52]

Example

The justification is appropriate in emergency situations. For instance, a student threatens to self-harm in a social media post. The institution would be justified in disclosing the student's personal information to the authorities to intervene.

3.3.2. Data subject's right to object

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'.[53] Data subjects must be informed of their right to object.[54] If a data subject objects, the institution may no longer process the personal information.[55]

Essentially, data subjects must be allowed to opt out of the processing of their personal information based on this justification. However, practically it can be difficult to achieve, which means that this justification should only be relied on if none of the other justifications apply.

3.3.3. When this justification does not apply

This justification is not appropriate when the processing activity involves large scale processing. It is more suited to unusual processing activities involving single or small numbers of records.[56]

In addition, this justification cannot be relied on to process special personal information.[57]

Justifying the processing of special personal information is discussed in part C, section 4.

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

3.4.1. The scope of this justification

[51] Section 11(1)*(d)*.
[52] Article 7(d) of the GDPR refers to the data subject's 'vital interest'.
[53] Section 11(3)*(a)*.
[54] Section 18(1)*(h)*(iv).
[55] Section 11(4).
[56] Article 29 Data Protection Working Party *Legitimate Interests* 20; Information Commissioner's Office *GDPR Guide* 74.
[57] It is not listed in section 27(1).

If the processing of personal information is necessary for the performance of a public law duty by a public body, the processing activity will be justified.[58]

Relevant section:

The definition of 'public body' in section 1.

The justification will also apply if the processing activity is necessary for the performance of a public power or function of another public body. For example, where the Department of Higher Education and Training requires information from universities in order to fulfil its mandate.

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 substance and fundamental objective of the public function.

3.4.2. Data subjects' right to object

When an institution relies on this justification, data subjects must be allowed to object to the processing activity at any time 'on reasonable grounds relating to his, her or its particular situation'.[59] Data subjects must be informed of their right to object.[60] If a data subject objects, the institution may no longer process the personal information.[61] Essentially, data subjects must be allowed to opt out of the processing of their personal information based on this justification.

However, as this can be difficult to achieve practically this justification should only be relied on if none of the other justifications apply.

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

3.5.1. The scope of this justification

The processing of personal information is justified if the activity is necessary for pursuing the legitimate interest of the responsible party, or of a third party to whom the information is supplied.[62] It is important here to distinguish between the responsible party's interest in the processing and the purpose of the processing activity. The purpose is the reason why the personal information is processed. The responsible party's interest is 'the broader stake that a [responsible party] may have in the processing, or the benefit the [responsible party] derives – or that society might derive – from the processing.'[63]

Examples of the legitimate interest of the responsible party

[58] Section 11(1)*(e)*.
[59] Section 11(3)*(a)*.
[60] Section 18(1)*(h)*(iv).
[61] Section 11(4).
[62] Section 11(1)*(f)*.
[63] Article 29 Data Protection Working Party *Legitimate Interests* 24.

The following are examples of interests that may be legitimate:

- an economic interest to learn as much as possible about its students so it can effectively intervene before a student fails;
- processing activities that are related to the performance of a contract or compliance with legislation that are strictly speaking not 'necessary;'[64]
- enforcement of legal claims including debt collection;
- preventing fraud or misuse of services;
- physical and cyber security;
- processing for historical, scientific, or statistical purposes; and
- employee monitoring for safety or management purposes.[65]

Examples of the legitimate interest of a third party

The following are examples of the interests of third parties that may be legitimate:

- if society has an interest in scientific research;
- if the disclosure of information (such as the salaries of top management in an institution) is aimed at improving transparency and accountability; and
- if it is in the public interest to take steps to combat illegal activity.[66]

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.[67] In other words, if the legitimate interest is not compelling (e.g. the interest in selling more products), the infringement of the data subject's privacy would have to be trivial for the responsible party's interest to be legitimate. This is referred to as a legitimate interest assessment.[68]

The following factors should be assessed in the legitimate interest assessment:

- The nature of the responsible party or third party's interest which will depend on whether

[64] Article 29 Data Protection Working Party *Legitimate Interests* 36.
[65] Article 29 Data Protection Working Party *Legitimate Interests* 25.
[66] Article 29 Data Protection Working Party *Legitimate Interests* 28.
[67] Article 6*(f)* of the GDPR contains a built-in balancing test. It provides that an institution cannot rely on the legitimate interest justification if 'such interests are overridden by the interest or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.' Therefore, the commentary on this provision of the GDPR does not carry the same weight as it would have if the provisions were identical.
[68] Information Commissioner's Office *GDPR Guide* 81.

- the interest in itself is a fundamental right (e.g. freedom of expression, the right to access to information);
- it is in the public interest;
- it is related to any of the other justifications;[69] or
- the legitimacy of the interest is recognised by law or by society.[70]

- The impact of the processing activity on the data subject which will depend on
  - the nature of the personal information (e.g. the sensitivity of the information);
  - the way in which the personal information is being processed (e.g. the scale of the processing, whether it is being disclosed to a large number of people in the process);
  - the reasonable expectations of the data subjects with regard to the use and disclosure of their personal information;
  - the likelihood and severity of any negative or positive consequences of the processing (including emotional impacts such as irritation, fear, distress); and
  - the relationship between the responsible party and the data subject (i.e. their relative resources and bargaining power, or whether the data subject belongs to a vulnerable segment of the population).[71]
- If there are any additional measures in place, such as:
  - strict limitations on how much personal information is collected;
  - the immediate deletion of the personal information that is used;
  - technical and organisational measures to keep the personal information secure;[72]
  - anonymising the personal information;
  - increased transparency; and

[69] Sometimes an institution will be unable to prove that the processing activity is 'necessary' for the performance of a contract or to comply with legislation, but it is still related to the contract or compliance. In such instances, the legitimate interest justification can be used.
[70] Article 29 Data Protection Working Party *Legitimate Interests* from 34.
[71] Article 29 Data Protection Working Party *Legitimate Interests* from 36.
[72] E.g. pseudonominisation or encryption.

- an easy to use opt-out.[73]

If the legitimate interest assessment identifies a significant privacy impact, a full privacy impact assessment should be conducted.[74] Privacy impact assessments are discussed in part D, section 3.

3.5.2. Data subjects' right to object

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'.[75] The data subjects must be informed of their right to object and [76] if they object, the institution may no longer process the personal information.[77]

Essentially, data subjects must be allowed to opt out of the processing of their personal information based on this justification. However, as this can be difficult to achieve practically this justification should only be relied on if none of the other justifications apply.

3.5.3. When this justification does not apply

This justification cannot be relied on to process special personal information.[78] Justifying the processing of personal information is discussed in part C, section 4.

3.6. Personal information may be processed with the consent of the data subject or a competent person where the data subject is a child

If the data subject or a competent person where the data subject is a child, consents to the processing, then the processing of personal information is justified.

'Child' is defined in section 1 of the POPIA as 'a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take action or to make decisions in respect of any matter concerning him- or herself'. Justifying the processing of the information of a child is discussed in part C, section 5.

Relevant section:

- The definition of 'consent' in section 1
- Section 11(2) (Burden of proof and the right to withdraw consent)

One of the biggest misconceptions about the POPIA is that consent is always required to legally process a data subject's personal information. While it is true that all processing activities must be legally justifiable, consent is just one of the listed justifications.

[73] Article 29 Data Protection Working Party *Legitimate Interests* from 41.
[74] Information Commissioner's Office *GDPR Guide* 82.
[75] Section 11(3)*(a)*.
[76] Section 18(1)*(h)*(iv).
[77] Section 11(4).
[78] It is not listed in section 27(1).

Consent should only be used as a justification if none of the other grounds are present for the following reasons:

- Consent must be voluntary.[79] This means that the data subject must be able to decline to give consent, without being excluded from the activity to which the processing relates (e.g. become a student or employee). When the processing is required by contract or by law, the data subject cannot withhold consent.

- The data subject has the right to withdraw consent at any time.[80] If the processing activity is required by contract or law, the responsible party will not be able to stop the processing activity without breaching the contract or failing to comply with the relevant legislation.

- Consents are very difficult and expensive to manage. It is up to the responsible party to prove when consent was provided, what the data subject consented to, the wording of the consent, etc.

3.6.1. Consent must be voluntary

In order to rely on this justification, the consent must be voluntary. This means that:

- The data subject must be given a genuine choice. Consent cannot be used as a justification where the processing activities are not optional or where a refusal of consent would mean that the institution cannot continue to provide services to or employ the data subject.[81]

- Consent may not be appropriate where there is a significant imbalance of power, for instance, in the employment relationship, employees may not be able to deny their employer consent.[82] If that is the case additional steps should be taken to assure the data subject understands that consent can be withheld.

- Consent must not be bundled with the acceptance of terms and conditions.[83] The data subject must have the freedom to withhold consent, but still conclude the contract.

- If the consent relates to multiple processing purposes, separate consent should be obtained for each processing purpose. In other words, the consent must be granular.[84]

- Data subjects must be free to withdraw consent without undue effort. It is considered best practice for the withdrawal of consent to be possible through the same channel that consent was obtained. For instance, if consent is obtained

[79] See the definition of consent in section 1 of POPIA.
[80] Section 11(2)*(b)*.
[81] Article 29 Data Protection Working Party *Guidelines on consent under Regulation 2016/679* 5.
[82] Article 29 Data Protection Working Party *Consent* 7.
[83] Article 29 Data Protection Working Party *Consent* 8.
[84] Article 29 Data Protection Working Party *Consent* 10.

through a user interface, the data subject should also be able to withdraw consent on the user interface.

- The institution must be able to demonstrate that data subjects who withheld or withdrew consent did not suffer any detrimental effects such as an increase in cost or a decrease in service levels.[85]

3.6.2. Consent must be specific

The consent must be specific to be valid. The consent must always relate to a specific processing purpose. A blanket consent to the processing of personal information will not be valid.

3.6.3. Consent must be informed

The consent must be informed. Data subjects must be given information about the consent before they make their decision. The consent must be drafted in clear, plain language and for this the institution must take the kind of audience the consent is aimed at into account. For instance, if the targeted audience are children, the institution must ensure that the information is understandable for minors.[86] This is discussed in further detail as part of the transparency requirement in part C, section 9.

3.6.4. Consent must be explicit

The consent must be explicit. This means that consent has to be given through a clear, unambiguous, affirmative act. Silence or inactivity cannot be taken as consent which is why the use of pre-ticked opt-in boxes is not allowed. To avoid ambiguity, the action of giving consent must be distinct from other actions such as agreeing to a contract. [87]

4. PROCESSING SPECIAL PERSONAL INFORMATION MUST BE AUTHORISED

Relevant section:

Section 26 (Prohibition on processing of special personal information)

If an institution processes special personal information, additional authorisation is required. This means that for the processing to be lawful, the processing must be justified on one of the grounds discussed in part C, section 3, and this section.

Special personal information is information that relates to:

- religious beliefs;

[85] Article 29 Data Protection Working Party *Consent* 10.
[86] Article 29 Data Protection Working Party *Consent* 14.
[87] Article 29 Data Protection Working Party *Consent* 16.

- philosophical beliefs;
- race;
- ethnicity;
- trade union membership;
- political persuasion;
- health;
- sex life;
- biometric information; or
- allegations of criminal behaviour or information that relates to criminal proceedings.

Institutions must identify special personal information because additional justifications for processing this information are required.[88] If no special justifications are present, the processing of special personal information is prohibited.

These special justifications are divided into:

- general authorisations that apply to all types of special personal information; and
- specific authorisations for different types of special personal information.

Institutions should:

- classify special personal information;
- determine and document which of the general authorisations the institution wants to rely on; and
- determine and document whether any of the specific authorisations apply.

4.1. General justifications for the processing of special personal information

Relevant section:

Section 27 (General authorisation concerning special personal information)

The general justifications for the processing of special personal information is discussed in the remainder of this section.

[88] Information classification is discussed in part C, section 10.

4.1.1. The establishment, exercise or defence of a right in law

A 'right in law' can be created by legislation, the common law, and even a contract. The same considerations would apply as those discussed in part C, sections 3.1 and 3.2. Due to the fact that the justification relates to special personal information, the Information Regulator will interpret it very narrowly.

4.1.2. International public law

Ordinary personal information can be processed if it is 'necessary for the proper performance of a public law duty by a public body'.[89] This was discussed in part C, section 3.4. The same considerations will apply here, with two significant differences:

- the justification in respect of special personal information is limited to the performance of international public law duties; and
- the justification is not limited to public bodies as is the case with other types of personal information.

In other words, institutions who are not public bodies may rely on this justification if they are complying with an obligation of international public law.

4.1.3. Historical, statistical, or research purposes

Although it is not explicit, it would appear that consent will generally be required before identifiable special personal information is used for research purposes. This is not unprecedented. Section 12(1)*(c)* of the Constitution provides that '[e]veryone has the right to bodily and psychological integrity, which includes the right … not to be subjected to medical or scientific experiments without their informed consent.'[90] The processing of health information, is discussed in part C, section 4.2.5.

The use of special personal information without consent for historical, statistical, or research purposes will be justified if:

- the processing is in the public interest; or
- it is impossible or would require a disproportionate effort to ask for consent; and
- sufficient guarantees have been provided to ensure that the processing does not adversely affect the privacy of the data subjects to a disproportionate extent.

Examples of historical, statistical, or research purposes that are in the public interest include research aimed at improving public health, crime prevention, and advancing the protection of human rights.

[89] Section 11(1)*(e)*.
[90] Medical or scientific experiments is research. See Department of Health *Ethics in Health Research: Principles, processes and structures* (2015) 8.

It is not an absolute requirement that the purpose for which the information is processed must be in the public interest. An institution will also be able to rely on this justification if it would require a disproportionate effort to ask for consent.

Institutions have to show that the processing of personal information is either in the public interest or it must have been too difficult to obtain consent. In addition, they must provide sufficient guarantees that the privacy of the data subjects will not be disproportionately affected. Sufficient guarantees may include:

- strict limitations on how much personal information is collected;
- the immediate deletion of the personal information that is used;
- technical and organisational measures to keep the personal information secure (e.g. pseudonymisation or encryption);
- anonymising the personal information;
- increased transparency; and
- an easy to use opt-out.[91]

4.1.4. The information has deliberately been made public by the data subject

Data subjects may deliberately make their personal information public on websites or on social media. Institutions often want to rely on this as a justification for collecting personal information. However, there are several reasons why this type of collection is dangerous. These are discussed in part C, section 8.2.2.

4.1.5. The data subject gave consent

The processing of special personal information can be justified by obtaining consent. The requirements for valid consent and the limitations of this justification are discussed in part C, section 3.6.

4.1.6. The information may be processed for health reasons

Special personal information may be processed if it is necessary to supplement information about the data subject's health in order for a medical institution to provide proper treatment or care.[92]

4.2. Specific justifications

Even if none of the justifications in section 4.1 apply, the POPIA allows for the processing of special personal information as it may be justified if one of the specific justifications exist.

[91] Article 29 Data Protection Working Party Legitimate Interests from 41.
[92] Section 32(4).

4.2.1. Religious or philosophical beliefs

Relevant section:

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

The processing of religious or philosophical beliefs will be allowed if:

- spiritual or religious institutions or institutions founded on religious or philosophical principles process information relating to the religious or philosophical beliefs of their members in order to achieve the institution's aims or principles; or
- another institution wants to protect the spiritual welfare of the data subjects, in which case, the data subjects must be given an opportunity to object.

For example

A university asks students to provide information about their religious beliefs to ensure that Muslim students are placed in residences where the kitchen is Halaal.

This will be justifiable as long as the students can decline to provide the information.

4.2.2. Race or ethnic origin

Relevant section:

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

Sometimes legislation requires the collection of the race or ethnic origin of data subjects. For instance, when the Employment Equity Act[93] requires that an employer collect the race of an employee.

4.2.3. Trade union membership

Relevant section:

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

If a data subject belongs to a trade union, then that trade union can process personal information relating to the data subject's membership if the processing is necessary to achieve its aims. The trade union may not share this personal information with third parties without the data subject's consent.

4.2.4. Political persuasion

Relevant section:

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

[93] Employment Equity Act 55 of 1998.

An institution founded on political principles can 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.

Political institutions may not provide information relating to a data subject's political persuasion without the consent of the data subject.

4.2.5. Health or sex life

Relevant section:

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

Information about a data subject's health or sex life may only be processed if the processing is necessary for:

- the proper treatment or care of a data subject by medical professionals, healthcare institutions or facilities, or social services;
- the administration of a healthcare institution, facility, professional practice, or social services;
- insurance companies, medical schemes, medical scheme administrators, and managed healthcare institutions to assess risk (unless the data subject has objected to this processing), to perform in terms of their agreement with the data subject, or to enforce any contractual rights or obligations;
- schools to provide special support for pupils or to make special arrangements in connection with their health or sex life;
- any institution to manage the care of a child;
- any public body to implement prison sentences or detention measures; or

- administrative bodies, pension funds, employers, or institutions working for them to

    - comply with laws, pension regulations, or collective agreements that create rights dependent on the health or sex life of the data subject, and

    - reintegrate or support workers or persons who are entitled to a benefit in connection with sickness or work incapacity.

Information about health or sex life must always be treated as confidential. If the responsible party 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, if it is required by law.

Information concerning inherited characteristics (i.e. characteristics controlled by genes) may only be processed if:

- a serious medical interest prevails; or

- the processing is necessary for historical, statistical or research activity.

The Information Regulator may make regulations

The Information Regulator may make regulations relating to the processing of health information in terms of section 32(6). In the draft Regulations which were published by the Regulator early in 2018, it called for interested parties to provide comments and inputs. The final regulations which were published in December 2018 did not contain any regulations relating to health information.

4.2.6. Criminal behaviour or biometric information

Authorisation concerning the data subject's criminal behaviour or biometric information.

(1) The prohibition on processing personal information concerning a data subject's criminal behaviour or biometric information, as referred to in section 26, does not apply if the processing is carried out by bodies charged by law with applying criminal law or by responsible parties who have obtained that information in accordance with the law.

(2) The processing of information concerning personnel in the service of the responsible party must take place in accordance with the rules established in compliance with labour legislation.

(3) The prohibition on processing any of the categories of personal information referred to in section 26 does not apply if such processing is necessary to supplement the processing of information on criminal behaviour or biometric information permitted by this section.

This restriction relates to criminal behaviour. Criminal behaviour refers to the alleged commission of any offence as well as information about any proceedings relating to that

offence.[94] 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.

Examples of personal information relating to criminal behaviour

The disciplinary records of students and employees may be seen as information relating to criminal behaviour depending on the offence in question.

Employers are entitled to process information relating to criminal behaviour as long as it does so in accordance with the rules established in labour legislation.

Any institution that processes information on criminal, unlawful, or objectionable conduct on behalf of third parties will require prior authorisation from the Information Regulator.[95]

5. PROCESSING THE INFORMATION OF CHILDREN MUST BE JUSTIFIED

Relevant section:

Section 35 (General authorisation concerning personal information of children)

The POPIA defines a child as 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.'[96]

Example

Examples of when a university will process personal information of a child is the processing of personal information:

- of prospective students;
- of applicants;
- of beneficiaries of employees; and
- for research purposes.

Children are inherently vulnerable, that is why the processing of their personal information is subject to additional restrictions.

5.1. Justifications for processing the information of children

[94] Section 26(b).
[95] Section 57(1)(b).
[96] Section 1 of the POPIA.

Personal information of children may be processed if the:

- parent or guardian consents to the processing of the child's personal information;
- processing is necessary for compliance with an obligation imposed by law;
- processing is necessary to comply with an obligation imposed in terms of international public law;
- processing is for historical, statistical, or research purposes; or
- personal information was deliberately made public by the child with the consent of the child's parent(s) or guardian(s).

These justifications are identical to the justifications for special personal information in section 27 and are discussed in part C Section 4.1.

Due to the many instances in which personal information of children are processed, there is a possibility that the Information Regulator will make regulations.

5.2. Age verification measures

The POPIA does not explicitly require that a responsible party must verify the age of data subjects. However, it is implicitly required that responsible parties should take steps to verify the age of data subjects whose personal information they are processing.

The measures implemented by institutions must be proportionate to the nature and risks of the processing activities.[97] Age verification should not lead to the excessive processing of personal information and the mechanism chosen to verify the personal information of the data subject must involve a risk assessment of the proposed processing.[98]

5.3. The definition of a competent person

The POPIA defines a 'competent person' as 'any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child.[99]

In other words, a competent person would be a person who has parental responsibilities in respect of the child. The Children's Act gives parental responsibilities to a parent and a legal guardian, and states that a parent or legal guardian must assist or represent a child in administrative, contractual, and other legal matters.[100] If a child has more than one guardian, it is possible for one of the guardians to exercise independently and without consent of the other guardian any right or responsibility arising from such guardianship.[101]

[97] Article 29 Data Protection Working Party *Guidelines on consent under Regulation 2016/679* 25.
[98] Article 29 Data Protection Working Party *Guidelines on consent under Regulation 2016/679* 25.
[99] Section 1 of the POPIA.
[100] Section 18(3)(b) of the Children's Act 38 of 2005.
[101] Section 18(5) of the Children's Act 38 of 2005.

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.[102]

A competent person can consent to the processing of personal information of a child. It is important to ensure that the person who is consenting is in fact the parent or legal guardian of the child. Measures must be put in place to verify this. What may be considered reasonable in deciding whether a person who is providing consent on behalf of a child is the holder of parental responsibility will depend on the risks inherent in processing personal information.[103] In low-risk cases verification can be done via email and in high-risk cases it would be appropriate for an institution to obtain proof that the person is the holder of parental responsibility over the child.[104] An institution must however apply the principles of the POPIA to the information it collects from the person when verifying him or her.

5.4. Prior authorisation may be required for cross-border transfer

An institution will require prior authorisation from the Information Regulator if the personal information of children is going to be shared with a third party in a foreign country that does not provide an adequate level of protection.[105]

6. SECONDARY PROCESSING PURPOSES MUST BE COMPATIBLE WITH THE ORIGINAL PURPOSES

Relevant section:

Section 15 (Further processing limitation)

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.

Further processing will be automatically justified if:

- the data subject consented to the new or changed purpose;
- the personal information was available in or derived from a public record or was deliberately made public by the data subject;
- further processing is required ‘to avoid prejudice’ to the maintenance of the law by any public body including the prevention, detection, investigation, prosecution, and punishment of offences;

[102] Section. 45(4) of the Children’s Act38 of 2005.
[103] Article 29 Data Protection Working Party *Guidelines consent under Regulation 2016/679* 26.
[104] Article 29 Data Protection Working Party *Guidelines consent under Regulation 2016/679* 26.
[105] Section 57(1)*(d)*.

- the processing is being done by the South African Revenue Services in terms of the South African Revenue Service Act;[106]

- the processing is necessary for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;

- the processing is in the interest of national security;

- the processing is aimed at preventing or mitigating a serious threat to public health or safety or the life or health of the data subject or another 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 the results will not be published in an identifiable form; or

- an institution applied to be exempted from the Information Regulator in terms of section 37.

If none of these automatic justifications exist, the institution must assess the general compatibility of the new or changed purpose to the original purpose. If the purposes are compatible, no new justification except for the one that justified the initial processing, is required. To do this, the following factors must be considered:

- The relationship of the new or changed purpose to the original purpose. If the new or changed purpose is very different from the original purpose or would be an unexpected change, it is unlikely that it is compatible.[107]

- The nature of the personal information concerned and the consequences of the processing activity. If the new or changed purpose would have a big impact on the data subject, it is unlikely that it is compatible.[108]

- The manner or context in which the personal information has been collected and the contractual rights and obligations between the institution and the data subject. This includes an assessment of the reasonable expectation of the data subject based on the nature of the relationship between the institution and the data subject.[109]

If the new or changed purpose is not compatible, the institution must determine a new justification for the processing activity. In other words, the institution must comply with part C, section 3.1 to 3.6 again and ensure that all other requirements in terms of the POPIA are met.[110]

[106] Act 34 of 1997.
[107] Information Commissioner's Office *GDPR Guide* 57.
[108] Information Commissioner's Office *GDPR Guide* 57. Recital 50 of the GDPR provides that the following activities are considered compatible: archiving in the public interest, scientific or historical research or processing for statistical purposes.
[109] Recital 50 of the GDPR.
[110] For instance, the transparency requirements must be complied with (see part C, section 9). This may require amendments to the relevant privacy notice and notification to the data subject before the further processing takes place.

7. PROCESSING MUST BE MINIMAL

Once it is established that a particular processing activity is justified in terms of section 11, the lawfulness of that processing activity will depend on the extent of the infringement on the data subject's privacy and whether the infringement is justified. The infringement will be justified if there is no less intrusive way to achieve the purpose of a processing activity.

In this section, the principle that the personal information must be adequate, relevant, and not excessive for the purpose for which it is processed, will be discussed.

7.1. The infringement of the data subject's privacy must be minimal

Relevant sections:

- Section 9 (Lawfulness of processing)
- Section 10 (Minimality)
- Section 13(1) (Collection for specific purpose)

All processing of personal information must be done in a reasonable manner.[111] To determine what is reasonable, the principle of minimality is considered.[112] This is also referred to as data minimisation.[113]

The principle of minimality states that personal information can only be processed if the personal information is:

- adequate,
- relevant, and
- not excessive,

considering the purpose of the processing activity.

7.2. The personal information must be adequate

The personal information used in a processing activity must be adequate to fulfil the purpose of that activity. Information will be inadequate if it is incomplete, out of date, or inaccurate. This means that an assessment of the adequacy of the personal information is also an assessment of the quality of the information. It is the responsible party's duty to take reasonable steps to ensure that personal information is complete, accurate, not misleading and updated where necessary.[114]

[111] Section 9*(b)*.
[112] Section 10.
[113] Information Commissioner's Office *GDPR Guide* from 27. Section 10 of the POPIA is very similar to article 5(1) of the GDPR. It is therefore appropriate to take guidance from the commentary on the GDPR.
[114] Section 16(1). Information quality is discussed in part C, section 12

7.3. The personal information must be relevant and not excessive

Information must be relevant. This requirement refers to the fact that the personal information collected must be appropriately connected to the purpose for which the information is being processed. If the personal information is not needed to achieve the purpose, the responsible party does not have the right to retain the information because it is not relevant.[115]

Sometimes personal information may have been relevant when it was collected, but is no longer relevant, because it is dated. For instance, the fact that a person was declared bankrupt 15 years ago, is no longer relevant when a responsible party wants to assess the person's ability to work with money. This is referred to as 'the right to be forgotten'.[116]

The fact that the information must not be excessive overlaps with the requirements that the information must be relevant. It emphasises the fact that responsible parties must guard against overcollection.

8. PERSONAL INFORMATION MUST COME FROM A LAWFUL SOURCE

Personal information must always come from a lawful source. In this section the default principle that personal information should be collected directly from the data subject, will be discussed. Any departure from this default principle must be justified.

To remain compliant with the POPIA, an institution must review all its collection practices regularly and keep a record of where personal information came from.[117]

8.1. Collecting information from the data subject

Relevant section:

Section 12 (Collection directly from data subject)

The default position is that personal information must be collected directly from the data subject. There are two main reasons for this:

- The responsible party can assume that the information is of a good quality.[118]

[115] Also see section 14(1) which provides that personal information must not be retained for longer than is necessary for achieving the purpose for which it was collected or subsequently processed. This is discussed in part C, section 14. Data subjects also have the right to demand that their personal information must be deleted (section 24(1)). This is discussed in part C, section 18.1.
[116] See *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* C-131/12. The decision in *Google Spain* 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 the 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, it is implicit in section 10.
[117] Section 17.
[118] Information quality is discussed in part C, section 12

- Data subjects will be aware that their information is being collected.[119]

Sometimes collecting personal information from other sources will be justified. This is discussed in the next section.

8.2. When collection from other sources will be justified

Although the default position is that personal information must be collected directly from the data subject, there are instances when it may be justified to collect personal information from another source.

Relevant section:

Section 12(2)

If any of these justifications apply, it is lawful to collect the personal information from a source other than the data subject. However, the use of this personal information must still be justified in terms of section 11. This is discussed in part C, section 3. It is entirely possible that there may be cases where the institution will be entitled to collect the personal information from another source but will not be entitled to use it.

Example

A university obtains the contact details of a former student on the personal website of the student. While the university is justified in collecting that information from the website, it cannot use that information for direct marketing unless they obtain the student's consent.

8.2.1. The personal information is in a public record

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

Relevant section:

The definition of 'public record' in section 1

To qualify as a public record in the public domain, the record must be:

- accessible to the public as a whole without being subject to any legal or other restrictions; [120] and
- in the possession or under the control of a public body.[121]

Examples of public records include the deeds registry, municipal rates and accounts, and information found at the Companies and Intellectual Property Commission (CIPC).

[119] The transparency requirement is discussed in part C, section 9
[120] English Oxford Living Dictionaries *'Public Domain'* accessed at https://en.oxforddictionaries.com/definition/public_domain, last accessed on 22 August 2018.
[121] See the definition of a 'public body' in section 1 of the POPIA.

8.2.2. The personal information has deliberately been made public by the data subject

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

In many cases institutions will want to rely on this justification for collecting personal information from websites or social media platforms. This is dangerous because:

- the data subject often did not make the information available, or the institution could not determine who made it available. For instance, collecting personal information will not be justified if someone else (i.e. the data subject's employer or a friend) made the personal information public; and

- the institution may not assume that the information is correct[122] or still relevant.[123] This means that the information must be verified before it can be used.

8.2.3. The use of another source is not prejudicial to the legitimate interest of the data subject

Personal information may be collected from another source if it is 'not prejudicial to the legitimate interest of the data subject'. The concept of 'legitimate interest' was discussed in part C, section 3.3. For instance, if a data subject is in physical danger, it may be justifiable to collect the personal information necessary to come to the aid of the data subject from whatever source is available.

8.2.4. The collection is necessary for law enforcement, national security, judicial proceedings, or tax collection

In certain instances, it is justified to collect personal information from a third party if the collection is necessary:

- to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution, and punishment of offences, or to comply with an obligation imposed by law;

- in the interests of national security;

- for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or

- to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Services Act.[124]

[122] part C, section 12
[123] part C, section 7.3
[124] Act 34 of 1997.

8.2.5. The collection is necessary to maintain the legitimate interests of the responsible party or of a third party to whom the information is supplied

The legitimate interest of the responsible party or third party must be weighed up against the rights and interests of the data subject to ensure that there is not a disproportionate infringement of privacy. There are certain factors to consider in the legitimate interest assessment. These factors are discussed in part C, section 3.3.

8.2.6. Collecting the personal information directly from the data subject would prejudice the lawful purpose of the collection

It may be justifiable to collect information from another source in instances where it is important to ensure that the information the institution obtained from the data subject is accurate. This becomes extremely important in instances where the data subject may be incentivised by the circumstances to provide inaccurate information.

Example

An institution obtains a report from a credit bureau to confirm that a student who applied for funding was truthful when declaring household income.

An institution may verify a prospective employee's degree with a verification agency to ensure that the employee meets the necessary requirements for the job.

8.2.7. The data subject has consented to the use of another source

The last justification for non-compliance with the principle of sourcing information directly from the data subject is consent. This justification should only be relied on if none of the other justifications apply or could be relied on. This is because the rules that apply to obtaining consent are onerous. Consent must be voluntary, specific and informed. Consent will be:

- voluntary if the data subject is able to decline to give consent;
- specific if it relates to a particular processing activity; and
- informed if the data subject were given a reasonable opportunity to object to the processing activity.

9. PROCESSING MUST BE TRANSPARENT

Responsible parties are required to be transparent about the processing of personal information. The requirement of transparency enables data subjects to understand how processing takes place and gives them a way of exercising control over their information.

The transparency requirement is usually met through the use of privacy notices. A privacy notice is a legal document that informs the data subject of the following:

- who collects the information;
- how the information is being collected;

- the purpose for which the information is collected;
- when the information will be shared;
- how the information is protected, and
- what the rights and responsibilities of the data subject are.

In this section, the following aspects will be discussed:

- when notification must be made;
- what must be included in the notification;
- how notification should be made; and
- when notification need not be made.

9.1. When notification must be made

Relevant section:

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

The general principle is that the data subject must be informed when personal information is directly collected from the data subject. Notification cannot take place after the fact.[125] For instance, if the collection is taking place via a web-based form, the privacy notice should be available 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 possible after collection.

What is a reasonably possible period?

A reasonably possible period is one month after the information was collected from the data subject.[126] The one-month period must be shortened if the information collected is being used to communicate to the data subject. An example of this type of communication is direct marketing. With direct marketing data subjects must be informed of the collection the first time they are communicated to if communication happens prior to the one-month expiration. However, if there is no communication to the data subject within the first month of collection then the requirement for notice within one-month after collecting the information must be adhered to.[127]

If the purposes for which personal information is processed change (also referred to as further processing or secondary use), the institution must update the privacy notice and proactively

[125] Article 29 Data Protection Working Party Guidelines on transparency under Regulation 2016/679 14.
[126] Article 14(3) of the GDPR. Also see Article 29 Data Protection Working Party *Guidelines on transparency under Regulation 2016/679* 15.
[127] Article 29 Data Protection Working Party Guidelines on transparency under Regulation 2016/679 15.

bring the changes to the attention of the affected data subjects before the further processing or secondary use starts.[128]

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

9.2. What notifications must be made

Relevant section:

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

The POPIA gives a list of information to provide to data subjects when their information is collected, this includes:[129]

- what information is collected;
- where the information is not collected directly from the data subject, the source from which it is collected;
- the name and address of the institution;
- the purpose for which the information is collected;
- whether the supply of information by the data subject is voluntary or mandatory;
- the consequence of failure to provide the information;
- any law authorising the collection;
- if the institution intends to transfer the information to a third country or international institution and the level of protection afforded there;
- the recipient or category of recipients of the information;
- the nature or category of the information;
- the right of access to the information;
- the right to rectify the information;
- the right to object to the processing of the information; and
- the right to lodge a complaint to the Information Regulator.

[128] Information Commissioner's Office *GDPR Guide* 98.
[129] Section 18(1).

9.3. How should notification be made

When drafting a privacy notice it is important to ensure that the notice is written in a clear and concise manner. In the European Union the requirement is that the notice must be given in a 'concise, transparent, intelligible, and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.' [130] 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.

The language must be appropriate for the intended audience.[131] If, for instance, a privacy notice is intended for prospective students, the fact that they are still minors without the same level of education and sophistication as an adult, should be considered. This means that institutions should identify the intended audience and determine their average level of understanding.

The privacy notices must be easily accessible. This means that the data subject should not have to look for the information, it should be immediately apparent where to find the privacy notices. The following is considered best practice:[132]

- On a website, provide a link to the privacy notice that is clearly visible on each page.
- For an app, make the privacy notice available before the app can be downloaded from the relevant online store and once the app is installed it must never be more than 'two taps away'.

There are different ways of presenting privacy notices, these include:[133]

- A layered approach: providing short notices that contain key privacy information that have additional layers of more detailed information.[134]
- Dashboards: preference management tools that inform data subjects how their information is being used and allow them to manage what is done with their data.[135]
- Just-in-time notices: these are relevant and focused notices delivered at the time of collecting individual pieces of information. The use of contextual pop-ups that activate

[130] Information Commissioner's Office Guide to the Privacy and Electronic Communication Regulation 97; Article 29 Data Protection Working Party Guidelines on transparency under Regulation 2016/679 8.
[131] Article 12(1). 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.
[132] Article 29 Data Protection Working Party Guidelines on transparency under Regulation 2016/679 8.
[133] Information Commissioner's Office Guide to the Privacy and Electronic Communication Regulation 97.
[134] Article 29 Data Protection Working Party Guidelines on transparency under Regulation 2016/679 17.
[135] Article 29 Data Protection Working Party Guidelines on transparency under Regulation 2016/679 17.

when a data subject fills in an online form or to use a chatbot interface to create an interactive privacy notice has become popular.[136]

- Icons: these are small symbols that indicate the existence of the type of information being processed.

- Mobile and smart device functionalities: this includes pop-ups, voice alerts, and mobile device gestures.

The following recommendations apply in the non-digital environment:

- In a hardcopy or paper environment: written explanations, leaflets, cartoons, infographics, or flowcharts.

- Telephonic environment: oral explanations by a person to allow questions or automated or pre-recorded information with options to hear more detailed information.

- Screenless smart technology or Internet of Things environments such as Wi-Fi tracking analytics: icons, QR codes, voice alerts, written information in set-up instructions, videos incorporated into digital set-up instructions, messages by SMS or email, and public information campaigns.

- Person to person: oral explanations or written explanations in hard or soft copy format.

- 'Real-life' environment (e.g. CCTV monitoring): visible signs containing the information.

9.4. Not notifying data subjects must be justified

Relevant section:

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

There are also instances when it is not required to inform data subjects that their personal information is being collected. If:

- the data subjects have given their consent, or in the case of a child a competent person has given consent, for non-compliance with the notification rule;

- compliance would prejudice their legitimate interests;

- non-compliance is necessary to avoid prejudice to the maintenance of the law, comply with an obligation imposed by law, conduct proceedings in any court or tribunal, or comply with the interest of national security;

- compliance would prejudice the lawful purpose of collection;

[136] Section 29 Data Protection Working Party Guidelines on transparency under Regulation 2016/679 8.

- compliance is not reasonably practicable in the particular case;
- the information will not be used in an identifiable form; or
- the information is going to be used for historical, statistical, or research purposes.

These exceptions will be discussed in the remainder of this section.

9.4.1. The data subject or a competent person where the data subject is a child has provided consent for the non-compliance

The requirement for a valid consent is that it must be a voluntary, specific, and informed expression of will. The requirements for valid consent was discussed in part C, section 3.6.

When considering this option, institutions must motivate why they think it is fair to choose this option instead of complying with the transparency requirement, and the motivation must be recorded.

9.4.2. Non-compliance would not prejudice the legitimate interests of the data subject as set out in terms of this Act

If non-compliance with the requirement of transparency would not prejudice the legitimate interest of the data subject, then the data subject need not be notified.

9.4.3. Non-compliance is necessary for the following reasons

There may be instances where non-disclosure is necessary to:

- avoid prejudice to the maintenance of the law;
- comply with an obligation imposed by law;
- conduct proceedings in any court or tribunal; or
- comply with the interest of national security.

The word ‘necessary’ should be given a narrow meaning. Whether not disclosing the processing activities is ‘necessary’ should be substantiated and must also be fair under the circumstances.

Example

If the data subject is engaged in alleged illegal activities, the disclosure of the processing of personal information as part of an investigation may be prohibited as it will undermine the investigation (e.g. when a person is suspected of money-laundering or the financing of terrorism the Financial Intelligence Centre Act 38 of 2001 prevents the responsible party from tipping the customers off that they are under suspicion).

9.4.4. Compliance would prejudice a lawful purpose of the collection

It would be acceptable not to comply with the notification rule if notifying the data subject would undermine the processing objective.[137]

Example

Employers have a legitimate interest in monitoring employees' communications, and behaviour in order to measure performance and for security purposes. In some instances, notifying employees that they are being monitored may undermine that purpose.

9.4.5. Compliance is not reasonably practical in the circumstances of the particular case

There may be instances when notifying the data subject would not be practical. However, the institution must still comply with the obligation to process personal information lawfully. See part C, section 3 for the lawful justifications for processing personal information.

10. INFORMATION CLASSIFICATION

Information classification is the process of assigning an appropriate level of classification to information to ensure that it receives an adequate level of protection.[138] Information classification is not required explicitly in the POPIA but 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 achieve POPIA compliance.

A separate classification for special personal information must be created. This is necessary as a different set of rules may apply to special personal information.[139]

Institutions should:

- have a process to identify all personal information in its possession; and
- distinguish personal information from special personal information.

11. KEEPING A RECORD OF PROCESSING ACTIVITIES

Relevant section:

Section 17 (Documentation)

The POPIA requires that the responsible party must document all processing activities. In addition, a responsible party will have to store information about its processing activities in order

[137] Article 29 Data Protection Working Party Guidelines on transparency under Regulation 2016/679 31.
[138] This definition is based on the concept governed by the International Organisation for Standardisation (ISO) ISO 27001 Information Security.
[139] Additional justification is required in order to lawfully process special personal information. This is discussed in part C, section 4.2.

to respond to requests for information from the Information Regulator when it investigates POPIA compliance.

During an investigation, institutions may need to know:

- when the personal information was collected;
- where the personal information was collected from (e.g. the data subject, a third-party source, a public record);
- why the information was collected from a source other than the data subject, if that is the case;
- how the personal information was collected, including the version of the form, privacy notice, contract, or consent that was used when the personal information was collected;
- what the personal information will be used for;
- what the justification is for collecting and processing the personal information (e.g. is it necessary for the performance of a contract, if it is required by a particular piece of legislation, or if the data subjects consented to the particular processing activity);[140]
- who has access to the personal information;
- who has accessed, used, changed, deleted, or done anything else with the personal information and why (e.g. employees who have amended the information);
- which third parties the information was shared with and why;
- whether the information has been sent to another country;
- whether the data subject has ever objected to the processing of the personal information;[141]
- if the data subject and the responsible party cannot reach an agreement about a request for the correction, deletion, or destruction of the data subject's personal information, the record of the personal information must indicate that a request was made, but that it was denied;[142] and
- what steps have been taken to verify the accuracy of the personal information.

12. INFORMATION QUALITY

[140] This is discussed in part C, section 3.
[141] part C, section 17.4.
[142] Insert cross reference to data subject participation

Relevant section:

Section 16 (Information quality)

Institutions must take reasonable steps to ensure that information is of a good quality. What is reasonable under the circumstances 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 responsible party 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 responsible party will not be entitled to assume that the information is correct, and the responsible party may be required to take steps to verify the information.

This section must be read with the section on the lawful sourcing of personal information.[143] The reliability of the source of the information will determine what steps the institution must take to ensure that the information is accurate. For instance, when personal information is obtained directly from the data subject, institutions are generally entitled to assume that the information provided is correct, particularly if the data subject was made aware of the consequences of providing incorrect information. When information is obtained from other sources, the institution must not assume that the information is correct, particularly if the information is used to make important decisions about the data subject.

For information to be considered to be of a 'good quality' it has to be:

- complete;

- accurate;

- not misleading; and

- updated when necessary.

12.1. The information must be complete

Information must be complete. This is very important when it comes to personal information being used to make decisions about the data subject, for instance, the information that is given on an application form; if this information is incomplete it may affect the student's application.

12.2. The information must be accurate

Accuracy refers to the correctness of the record. Whether an institution must take active steps to keep personal information up to date will depend on the purpose for which it is used and the severity of the consequences 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 a university. It would be reasonable for the university to ask these data

[143] Part C, section 8.

subjects to update their details, but the university does not have to take more extreme measures such as independently verifying the 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.[144]

12.3. Information must not be misleading

If information is not kept up to date, the information provided may be misleading. This may have dire implications for data subjects and may affect the service that is offered to them.

For instance, opinions about a person are considered to be personal information. Opinions are inherently subjective and not intended to record matters of fact. This means that even if the 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 make it clear that it is an opinion and, where appropriate, whose opinion it is.[145]

12.4. Information must be updated when necessary

In order 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. What those steps should entail will depend on the circumstances, the type of personal information involved, and the purpose for which it was used.

Data subjects have the right to contest the accuracy of their personal information. When data subjects object to the accuracy of their information the institution is entitled to verify whether the data subjects' objections have merit and may decline to change the personal information if there is no merit. The personal information must not be processed while the institution is considering the update.[146]

It is not the data subjects' 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 address or indicate in its records that it is no longer current.[147]

12.5. Verifying or updating personal information from sources other than the data subject

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 the institution. For instance, a university may use public

[144] The retention of records is discussed in section 14 below.
[145] For more information on the treatment of opinions, see Information Commissioner's Office *GDPR Guide* from 34.
[146] Part C, section 17.4.
[147] Information Commissioner's Office *GDPR Guide* 36.

records to improve the quality of the contact details it has of its alumni or instruct a third party to do so on its behalf.

It will be justified if the institution wants to verify personal information that the institution already has or if the institution wants to improve the accuracy of the information as long as the use of a source other than the data subject is justified on one of the grounds in section 12(2). This was discussed in part C, section 8.2. 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 record individually, or because the contact details for the data subject is out of date.[148]
- 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.[149]
- the verification of the personal information from another source is necessary to maintain the legitimate interest of the third party.[150]
- the institution has the consent of the data subject to verify the information.[151] The most common example of this is when consent is requested to do 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. In particular, verification of information obtained from sources other than the data subject will be required if inaccuracies could have serious implications for the data subject. For instance, the financial information that is considered in order to decide whether to give a student funding should be both independently verified and confirmed by the data subject.

13. INFORMATION SECURITY

13.1. Reasonable security measures

Relevant section:

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

Institutions must safeguard personal information against:

[148] Section 12(2)*(f)*.
[149] Section 12(2)*(a)*.
[150] Section 12(2)*(d)*(iv).
[151] Section 12(2)*(b)*. The requirements for valid consent were discussed in part C, section 3.6.

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

Some examples of information security breaches:

- Unauthorised access by hackers or identity thieves.
- Accidental unauthorised disclosure of information, e.g. sending it to the incorrect recipient.
- Loss of access to personal information due to malicious software or the theft of information.
- Unauthorised access by staff members.
- Damage to, loss of, or loss of access to information through fire, floods, power outages, social unrest, unreliable storage (the management of this risk is often referred to as business continuity management).
- Destruction of personal information contrary to retention and disposal policies.
- Use of or sharing of personal information for unjustified purposes.
- Altering personal information without permission.

The POPIA requires that there be both technical and organisational measures to protect personal information. Examples of technical measures are firewalls, anti-virus software, encryption software, de-identification, and pseudonymisation.[152] Organisational measures include policies, procedures, clear descriptions of roles and responsibilities, and training.

The security measures required by the POPIA are based on a reasonableness standard. What is reasonable will depend on:

- the sensitivity of the information, which underscores the need for information classification;[153]

[152] De-identification and pseudonymisation are discussed in part B, section 1.1.
[153] This is discussed in part C, section 10.

- the extent of harm that compromised information could cause the data subject;
- the availability of technical and organisational measures to remedy the risk; and
- the affordability of the technical and organisational measures to remedy the risk.

In order to demonstrate that it behaved reasonably under the circumstances, an institution must be able to demonstrate that it has taken steps to:

- identify all reasonably foreseeable internal and external threats to personal information in its possession or under its control;
- establish and maintain appropriate safeguards against the threats identified;
- regularly verify that the safeguards are effectively implemented; and
- ensure that the safeguards are continually updated in response to new threats or deficiencies in previously implemented safeguards.

Information security guidelines

In order to comply with this section institutions should:[154]

- have information security policies (or equivalent) and take steps to ensure that they are implemented and that controls are in place to enforce them;
- undertake an analysis of the risks inherent in the processing of personal information, and use this analysis to assess the appropriate level of security required;
- keep a complete record of the decisions made about security measures to implement as well as the reasons for the decision;
- take generally accepted information security standards and procedures (e.g. ISO 27001, Cobit) and the cost of implementation into account when deciding what measures to implement; and
- regularly test and review their information security policies and measures and, where necessary, improve them.

13.2. Responsibility for operators

Relevant sections:

- Section 20 (Information processed by operator or person acting under authority)
- Section 21 (Security measures regarding information processed by operator**)**

[154] Information Commissioner's Office *GDPR Guide* 208.

Responsible parties may be held liable for the information security breaches of their operators. How to distinguish an operator from a responsible party is discussed in part C, section 1.

Sharing personal information and managing operators are discussed in part C, section 16.

13.3. Information security breach notification

Relevant section:

Section 22 (notification of security compromises)

The POPIA requires that a responsible party must notify the Information Regulator and data subjects in case of unauthorised access to personal information.

The notification duty is limited to unauthorised access or acquisition

The Information Regulator and data subjects only need to be informed of security breaches that involve the unauthorised access to, or acquisition of personal information, by an unauthorised person. While other security incidents relating to (for instance), the integrity of personal information ought to be managed, the Information Regulator and data subjects need not necessarily be notified.

The notification must meet the following requirements:

- The notification must take place as soon as reasonably possible after the security incident is discovered.

- The notification must not compromise the ability of law enforcement (or another public body) to investigate the breach or the ability of the responsible party to determine the scope of the incident and to restore the integrity of the responsible party's information system. In other words, there may be circumstances when it is necessary to keep the incident confidential while it is being investigated.

- The notification must be in writing and must be communicated through at least one of the following communication channels: by post, by email, announced in a prominent position on the responsible party's website, published in news media or any other channel determined by the Information Regulator.

- The notification must contain enough information to allow data subjects to take steps to protect themselves against the consequences of the security breach. The notice must include a description of the possible consequences of the breach, measures the responsible party will take to address it, recommendations for the measures the data subject can take to minimise the effect of the breach, and the identity of the unauthorised person(s) who may have accessed or acquired the information.

13.4. Information security breach management

In order to discharge the duty to notify the Information Regulator and data subjects of data breaches, institutions should create and implement an incident management policy and procedure.[155]

14. RETENTION PERIODS

Relevant section:

Section 14 (1) to (3) (Retention and restriction of records)

Personal information must not be retained for any longer than is necessary to achieve the purpose of collection. However, there are instances in which an institution can justify retaining the information for longer periods. These justifications include:

- Retaining the information because it is required by a piece of legislation.
- Retaining the information because the institution requires the information for lawful purposes related to its functions or activities.
- Retaining the information as it is required by a contract between the parties.
- Retaining the information because a data subject, or a competent person in the case of a child, consents to the retention.
- Retaining the information for historical or research purposes. This is allowed as long as safeguards are put in place that prevent the records from being used for any other purpose.
- Retaining the personal information to use it to make a decision about a data subject. The information must be retained for any period required or prescribed by law, or if no period is prescribed then the period required in the context to give the data subject reasonable opportunity to request access to the record.

An institution must destroy personal information as soon as reasonably practicable after it no longer has any justification to retain it. Personal information is considered destroyed if it cannot be reconstructed in an intelligible form again.

15. RESTRICTION OF PERSONAL INFORMATION

Relevant section:

Section 14(4) to (8) (Retention and restriction of records)

[155] See the discussion of different types of security breaches in part C, section 13.1.

Institutions must have the ability to restrict processing personal information in the following circumstances:

- If the data subject is contesting the accuracy of the information, the processing must be restricted while the institution investigates the accuracy of the information.
- If the institution no longer needs the personal information to achieve the purpose for which it was collected but is retaining it as proof or for historical purposes, the institution must not process the personal information for any reason.
- If the institution was processing the personal information without a lawful justification, the data subject can request that the information must be restricted instead of being destroyed.
- If the data subject requests that the information be transmitted to another automated processing system, the processing of that personal information must be restricted.

What does restriction mean?

When personal information has been restricted, the institution may only store it or use it for proof. However, the restriction will be lifted if:

- processing the information is in the public interest;
- the information is being processed for the protection of another data subject; or
- the institution has the data subject's consent to resume processing.

16. SHARING AND THIRD PARTIES MUST BE MANAGED

Managing the sharing of personal information is a pivotal part of POPIA compliance. Many sharing activities may require consent as other justifications for lawful processing are often not present.[156]

This section applies to the sharing of personal information between:

- different universities;
- universities and funders;
- universities and researchers;
- universities and government departments;
- universities and other third parties (e.g. service providers); and

[156] See sections 11 and 15.

- once-off requests for access to single records (e.g. when a parent requests access to their child's personal information).

What is a third party?

In this section, the individual or institution with whom the information is shared will be referred to as a third party.

This section does not apply to:

- The collection of personal information from a third party. The collection of personal information from sources other than the data subject is discussed in part C, section 8.2. It is also discussed in the context of improving the quality of the information the institution already has in part C, section 12.5.

- Once-off requests for access to the personal information of a data subject(s) concerns governance by the Promotion of Access to Information Act which is discussed in part C, section 17.2.

The following topics will be discussed:

- accountability for shared information;

- justification for sharing information;

- transfer of information to other countries;

- secure transfer of personal information;

- linking and the use of unique identifiers;

- contractual requirements; and

- once-off requests for access to a single record.[157]

16.1. Identification and risk-rating of information sharing

This section applies to any sharing of personal information regardless of whether the personal information is actually transmitted to the third party or if the third party is given access to the institution's data base.

Before sharing personal information, it is good practice to perform a privacy impact assessment. This will help the institution identify the potential positive or negative effects of the sharing activity. This in turn will determine what level of governance is reasonable under the circumstances. For instance, if the sharing is high risk, more stringent information quality and security requirements may be warranted.[158]

[157] Sections 20 and 21.
[158] Information Commissioner's Office *Data sharing code of practice* 27.

Institutions should develop their own privacy impact assessments and the policies and procedures to ensure that the assessments are performed.

16.1.1. Accountability for shared information

When institutions share personal information, it is crucial to determine the nature of the relationship between the institutions. For purposes of this section we will refer to the institution who is sharing the information as ‘institution A’ and the institution who is given access to the information as ‘institution B’.

One of the following scenarios will apply:

- Institution A is the responsible party and is using institution B as an operator.
- Institution A and institution B are both responsible parties.
- Institution A is an operator and is using institution B as a sub-operator.

How to distinguish between a ‘responsible party’ and an ‘operator’ was discussed in part C, section 1.

Institutions should:

- identify the responsible party, operator or sub-operator for each instance of sharing;
- ensure that the contract between the parties accurately identifies the responsible party, operator, or sub-operator for each instance of sharing; and
- ensure that the contract accurately reflects who is responsible for compliance with this Code.

16.2. Justification for sharing information

The sharing of personal information with a third party must be justified. Justification was discussed in part C, section 3. Whether a particular instance of sharing is justified will depend on the purpose for which the responsible party was collecting the personal information, and whether sharing the information with the third party was necessary to achieve that purpose.

There is a difference in justifying the sharing of personal information between when the institution is sharing it with another responsible party and when it is sharing the information with an operator:

- When sharing the information with another responsible party, the institution must first establish whether the purposes for which the information is being shared is justified in terms of section 11.

An example: Sharing information with the government

Universities are often required to share information with the government. Even though it is the government requesting the information, section 11 must be applied. In many instances, sharing the personal information will be necessary to comply with legislation such as the Higher

Education Act[159] or the sharing will be necessary for the proper performance of a public law duty. [160]

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

- What is the purpose(s) 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 101 of 1997.

- Can the government justify using the personal information for those purposes? The Department's justification will also be that it is complying with legislation.

If the purpose for which the Department wants to use the personal information goes beyond complying with the Higher Education Act, that purpose must be justified on one of the other grounds. If sharing can only be justified on the basis that the Department is protecting a legitimate interest of the data subject, that the Department is exercising a public duty, or that it is in the Department's legitimate interest, the student will have the right to object to the sharing of the personal information.[161] The student must be informed of this right. In the alternative, the Department could ask for the student's consent, but in that case, the student will have the right to withdraw consent.

- When sharing the information with an operator, the question is whether the task the operator is going to perform on behalf of the institution is justified.

An example: Sharing personal information with service providers

A student applies for admission to a university, the student has to supply personal information that is necessary for the university to perform in terms of the contract with the student. The university makes use of a cloud service provider to store the personal information of students. In this example, the university is the responsible party, and the cloud service provider is an operator. As long as the reason for sharing remains the performance of the contract, sharing information with an operator will be justified.

If the purpose for sharing is not necessary to achieve the original purpose for which the responsible party was collecting the personal information, the sharing of the information will be considered as 'further processing' or secondary use. The further processing must be compatible with the original purpose for collection. This is discussed in part C, section 6.

When considering whether a particular sharing activity is justified, institutions should:

- document both its own purpose for sharing the information as well as the purposes for which the third party will use the personal information; and

[159] 101 of 1997 .
[160] See part C, section 3.2.
[161] See part C, section 3.3.2.

- document what justification the institution is relying on to legitimise the sharing.

16.3. Sharing must be minimal

The principle of minimal processing is discussed in part C, section 7. In the context of sharing, institutions must:[162]

- evaluate whether the sharing of personal information is necessary at all or whether the personal information can be de-identified; and
- ensure that only the minimum amount of personal information is being shared and the minimum number of institutions, and their staff members, have access to it.

16.4. Sharing must be transparent

The principle of transparency is discussed in part C, section 9.

Privacy notices must be reviewed regularly to ensure that they still accurately reflect the arrangements for sharing personal information.

It will not be practical to list the actual institutions with whom personal information is shared. Instead, institutions should provide a description of the types of institutions with which personal information is shared.

16.5. The quality of the information being shared

Institutions must take reasonable steps to maintain the quality of the personal information they hold, particularly if the information will be shared. The sharing of low quality or incomplete information can have severe implications for data subjects.

The following issues should be considered:[163]

- Is it clear who is responsible for maintaining the quality of the personal information?
- Is the format of the personal information compatible with the systems used by both institutions?
- Was the accuracy of the personal information checked before it was shared?
- Are there procedures in place to ensure that inaccurate personal information is corrected by all the institutions holding it?
- Have common retention periods and deletion or de-identification arrangements been agreed?

16.6. Secure transfer of information

[162] Information Commissioner's Office *Data sharing code of practice* (2011) 32.
[163] Information Commissioner's Office *Data sharing code of practice* (2011) 27.

The method by which information is shared must be secure. Inappropriate security measures can lead to the loss of information or unauthorised disclosure and can affect the integrity and availability of information.

16.7. Linking of information and the use of unique identifiers

Relevant section:

The definition of 'unique identifier' in section 1

When 'unique identifiers' are processed for purposes of linking the data sets held by different responsible parties, the institution(s) may require prior authorisation from the Information Regulator.[164]

16.8. Transfer of personal information to other countries

Relevant section:

Section 72 (Transfer of personal information outside the Republic)

If personal information is shared with an institution in another country, additional rules apply to ensure that the personal information enjoys equal protection outside of South Africa.

Personal information may only be shared with an institution in another country if:

- That country has data protection legislation that provides an adequate level of protection which is substantially similar to the POPIA and which also includes a section on further transfer of the information to other countries.

- The institution is bound by 'binding corporate rules' that provide an adequate level of protection which is substantially similar to the POPIA, and which also includes a section on the further transfer of the information to other countries. An example of this is where a company is bound by policies that govern data protection.

Relevant section:

The definition of 'binding corporate rules' in section 72

- The institution is bound by an agreement that provides an adequate level of protection that is substantially similar to the POPIA and which also includes a section on the further transfer of the information to other countries.

- The data subject has consented to the transfer.[165]

[164] Section 57(1)(a)(ii).
[165] The consent must be an informed, specific and voluntary expression of will and the data subject must be allowed to withdraw consent. See the discussion on consent in part C, section 3.6.

- The transfer of the personal information is necessary for the performance of a contract between the data subject and the responsible party or a third party, or for the implementation of pre-contractual measures taken on instruction from the data subject.[166]

- It was not practical to obtain consent, but the transfer is to the benefit of the data subject and if it were possible to ask consent, the data subject likely would have consented.

16.9. Contractual requirements

16.9.1. Between responsible parties

When responsible parties share personal information 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 will be adopted by the various institutions involved in the sharing operation.

A personal information sharing agreement should document the following aspects of the sharing activity:[167]

- The purpose(s) of the sharing: It must be clear for what purposes personal information may be shared and what purposes shared personal information may be used for.

- The justification for sharing: The agreement should indicate what justification exists for the sharing activity. If consent is the basis for sharing, the agreement should contain a model consent form.

- The personal information to be shared.

- Who will have access to the personal information: The personal information sharing agreement may include ‘permissions’ which will ensure that only certain members of staff have access to the information. The agreement may also require that those members of staff who will have access have received appropriate training.

- Quality assurances: The agreement may require periodic sampling exercises to ensure that the personal information being shared is accurate.

- The security of shared personal information: The agreement should prescribe common technical and organisational security arrangements, including for the transmission of the personal information as well as procedures that should be followed in the event of a breach.

- Retention of the shared information.

[166] This is similar to the general justification for the processing of personal information which was discussed in part C, section 3.1.1.
[167] Information Commissioner’s Office *Data sharing code of practice* 2011 26.

- Procedures to deal with access requests, queries, and complaints.
- The right to audit compliance with the agreement.
- How often the agreement will be reviewed.
- The consequences of breaching the agreement.

If personal information is being transferred to another country, the agreement should also contain a clause forcing the institution to comply with the POPIA. This is not always a requirement, because there are other justifications that may apply.[168]

16.9.2. Sharing with operators

Relevant sections:

- Section 20 (Information processed by an operator or persona acting under authority)
- Section 21 (Security measures regarding information processed by an operator)

If the institution is sharing personal information with an operator, a written operator agreement must be concluded. This agreement must contain the following clauses that:

- comply with the Protection of Personal Information Act;
- establish and maintain adequate security measures to prevent the loss of, damage to, unauthorised destruction of, unlawful access to, or unlawful processing of personal information;
- ensure confidentiality of the personal information;
- do not allow the processing of personal information without the responsible party's knowledge or authorisation; and
- notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by an unauthorised person.

If personal information is being transferred to another country, the agreement should also contain a clause forcing the institution to comply with the POPIA. This is not always a requirement, because there are other justifications which may apply.[169]

[168] See part C, section 16.8.
[169] See part C, section 16.8.

It is recommended that the agreement should also contain the right to audit compliance with the agreement.

16.10. Access to information requests by third parties

This section deals with requests for access to personal information by a third party that are not governed by a contract between the institution and the requestor. These requests are subject to the Promotion of Access to Information Act which is discussed in the part C, section 17.1.

17. ACCESS TO INFORMATION MUST BE MANAGED

There is an inherent tension between protecting the privacy of data subjects and the protection of the right to access information held by public and private bodies. Access to information is governed by the Promotion of Access to Information Act. This section will consolidate the POPIA and the Promotion of Access to Information Act.[170]

17.1. Data subject's access to their own information

17.1.1. The right to access

Relevant section:

Section 23(1) (Access to personal information)

The POPIA states that data subjects are entitled to:

- confirmation (free of charge) of whether the institution has their personal information;
- request a record or a description of the personal information the institution has; and
- know the identity of all third parties, or categories of third parties who have, or have had, access to the personal information.

It is important that data subjects are given access to their personal information:

- within a reasonable time;
- at a prescribed fee, if any;
- in a reasonable manner and format; and
- in a format that is understandable.

[170] Section 23.

Data subject requests make institutions vulnerable

Before an institution can grant a request for a record of or a description of personal information, the data subject's identity should be verified. The reason for this is that identity thieves often obtain personal information by pretending to be an individual requesting access to their own information.

Institutions should develop processes to confirm the identity of requesters before access is given to personal information.

17.1.2. The format of the access request

Relevant section:

Section 25 (Manner of access)

The same formalities that applied to requests for access to information in terms of the Promotion of Access to Information Act prior to the POPIA will apply.

17.1.3. Fees for access requests

Relevant section:

Section 23(3) (Access to personal information)

Institutions may charge a fee for access requests. However, they may not charge a fee if the data subject is simply confirming whether the institution has any personal information about them.

Institutions must provide a written estimate before providing access. They may require the payment of a deposit.

17.1.4. When an access request by the data subject can be denied

Relevant section:

Section 23(4) (Access to personal information)

Access requests by data subjects must be considered against the grounds for refusal of access to records in the Promotion of Access to Information Act. Different grounds for refusal exist depending on whether the institution is a public body or a private body. Some of the grounds are mandatory and others are discretionary (i.e. the institution may refuse or grant access).

17.2. The right to correct the information

Relevant section:

Section 23(2) (Access to personal information)

If personal information is provided to the data subject, they must also be informed of their right to request that the information be corrected. This right is discussed in part C, section 18.1.

17.3. Access requests by third parties

Sometimes, a third party will request access to the personal information of a data subject. For instance:

- a prospective employer may contact a university to verify that a degree was awarded to a job applicant;
- a bank contacts the university to confirm the employment of an employee who has applied for a loan; or
- a parent or a third party funding a student wants access to the academic record of an adult child.

In the case of a public university, whether to grant access or not will depend on section 34 of the Promotion of Access to Information Act.

Relevant section:

Section 34 of the Promotion of Access to Information Act (Mandatory protection of privacy of third party who is natural person)

The default rule is that an institution must only disclose information of someone other than the requester if it is reasonable to do so. Section 34(2) lists several exceptions to this default rule:

- The data subject consented to the disclosure. Section 48 of the Promotion of Access to Information Act simply provides that the consent must be in writing. The POPIA imposes additional requirements for a consent to be valid. This was discussed in part C, section 3.6.
- The data subject was informed that their personal information would or might be made available to the public.
- The personal information is already publicly available.
- The requester is providing medical treatment to the data subject and the data subject is over the age of 18 years and cannot provide the information themselves and providing the information is in the data subject's best interest.
- If the data subject is deceased. When this is the case the POPIA does not apply to the request.[171]
- If the data subject is an official of a public body and the information requested relates to the person's position or function, their contact details at work, information relating to their remuneration and their job description, or if the data subject's name appears on a record the data subject created in the course of their employment.

Relevant section:

[171] POPIA only applies to living individuals. See part C, section 1.1.2.

The definition of an 'official' in section 1 of the Promotion of Access to Information Act

All of the other principles of the POPIA will also apply to the sharing activity. For instance, the minimum amount of information must be shared, and the transmission of the personal information should be secure.

Access can also be denied if the requester cannot prove their identity.

Verification of a student's academic record to a prospective employer

Prospective employers often request that universities confirm that a student has been awarded a degree. If the student gave consent to the disclosure, the university can provide confirmation.[172]

A bank wants to verify employment

Banks need verification of the employment status of a person who has applied for a loan or credit. Section 34(2)(*f*) of PAIA provides that the University can disclose information relating to an employee's employment status and even their salary scale without consent.

17.4. New requirements for Promotion of Access to Information Act manuals

Section 14 of the Promotion of Access to Information Act provides that public bodies must have a PAIA manual. This requirement has been restated in the final POPIA regulations.

Can the Promotion of Access to Information Act manual also be the privacy notice?

The extensive transparency requirements imposed by the POPIA is discussed in part C, section 9. As long as both the requirements of section 18 of the POPIA as well as section 14 of the Promotion of Access to Information Act are met, the same disclosure can achieve compliance with both acts.

18. DATA SUBJECT RIGHTS

18.1. The right to correct, destroy or delete personal information

Relevant section:

Section 24 (the right to correct personal information)

Data subjects, in addition to having access to their personal information, also have the right to request that an institution: [173]

- corrects or deletes any personal information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully; or

[172] Technically PAIA provides that as long as you disclose that you will share the information with the prospective employer, you can share it. It doesn't fit 100%, because that exception refers to information that is provided by the data subject, not created by the institution ('insofar as it consists of information … that was given to the public body by the individual'). See section 34(2)(b).
[173] Section 24(1).

- destroy or delete a record that it is no longer authorised to retain. See discussion at part C, section 14.

Data subjects must request any of the above in the prescribed form and when the institution receives the request the institution must, as soon as reasonably practicable:[174]

- correct the information;
- destroy or delete the information; or
- provide the data subject with credible evidence in support of the information.

If the data subject's request is not granted because an agreement cannot be reached with the institution, the data subject may request that the institution take reasonable steps to attach to the information an indication that a correction of the information was requested but that it was not made.[175] The attachment to the information must be made in such a way that it will always be read with the information.[176]

An institution must always inform a data subject what action has been taken as a result of the data subject's request. [177]

An institution will deny this request in instances where the information must be retained. Information will be retained when: [178]

- it is required or authorised by law;
- the institution reasonably requires the record for lawful purposes related to its function or activities;
- it is required by a contract between the parties; or
- the data subject or a competent person where the data subject is a child has consented to the retention of the record.

See discussion at part C, section 14.

If a data subject contests the accuracy of the information, an institution must restrict the processing of that personal information for a period that will enable the institution to verify the accuracy of the information.[179]

18.2. The right to object to processing of personal information

Relevant section:

[174] Section 24(2a–c)
[175] Section 24(2)(d).
[176] Section 24(2)(d).
[177] Section 24(4).
[178] Section 14(1).
[179] Section 14(6)(a).

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

Data subjects may at any time object to the processing of their personal information. This objection may take place upon reasonable grounds that relate to the particular situation, unless legislation provides for such processing of personal information.[180] Data subjects may also object to the processing of personal information if the processing is used for the purposes of direct marketing by means of unsolicited electronic communication. [181]

Objections to the processing of personal information must take place in the prescribed manner.[182] The prescribed manner is set out in the POPIA Regulations of the POPIA.[183]

19. USE OF IDENTIFIABLE PERSONAL INFORMATION IN SCIENTIFIC RESEARCH

The POPIA applies to research activities involving identifiable personal information. While the provisions arguably makes sense for research that institutions would undertake to operate as a public university (e.g. institutional planning), they are not well suited to regulating scientific research.

Scientific research involving identifiable personal information will usually fall within the definition of 'health research' which is governed by the National Health Act.

The Ethics in Health Research Guidelines definition of 'health research'

'"Health research" per the NHA may be understood to include, but is not limited to research that contributes to knowledge of:

- biological, clinical, psychological, or social welfare matters including processes as regards humans;
- the causes and effects of and responses to disease;
- effects of the environment on humans;
- methods to improve health care service delivery;
- new pharmaceuticals, medicines, interventions and devices; and
- new technologies to improve health and health care.'[184]

The Ethics in Health Research Guidelines do contain some references to the POPIA. It states that:

[180] Section 11(3)(a).
[181] Section 11(3)(b).
[182] Section 11(3).
[183] Regulations Relating to the Protection of Personal Information, 2018.
[184] Ethics in Health Research: Principles, Processes and Structures (2015), paragraph 1.1.3.

'The Protection of Personal Information Act 4 of 2013 (partially in effect) has increased the need to ensure computer safety, locked record storage facilities and careful gate keeping about access to raw data including completed informed consent documents (see also 3.1.8). Researchers should take measures to ensure privacy and confidentiality interests throughout the research period, including when disseminating results or findings.'[185]

The specific implications of the POPIA is summarised as follows:

'The Protection of Personal Information Act 4 of 2013 was assented to on 19 November 2013. This Act provides guidance on how the right to privacy regarding personal information is protected. It stipulates that the right to privacy includes "protection against unlawful collection, retention, dissemination and use of personal information" (Preamble to Act). A tension between the right to privacy and the need for the free flow of information in a society that seeks to make progress on economic, social, health care and education fronts, is immediately evident. The Act does not appear to hold out negative implications for research activities that record personal information about research participants. However, special attention should be given to ensuring that computers and electronically stored data are protected from unauthorised access, inadvertent or accidental dissemination and distribution in the form of a 'data dump' etc.

Research activities are a legitimate purpose, provided that protective measures are adhered to. Thus, researchers and RECs should pay careful attention to measures that will protect privacy and confidentiality interests. In general terms a person should know what information is being collected, why it is being collected, what will happen to it, how long it will be retained, whether it will identify the person, whether it will be shared with others and why, whether it will be sent outside South Africa and why. The person should agree to these terms.

Some specific terms are summarised:

- in the case of a child (person under the age of 18 years), a parent or guardian must give permission for the information to be collected (s 35(1)(a));
- if the information is to be sent outside the Republic, the recipient must assure that the level of protection afforded in that country is commensurate with that expected in South Africa (s 18(1)(g));
- information about a person's race or ethnic origin must be necessary (s 29(a)) or for affirmative action purposes (section 29(b));
- information about a person's health or sex life must be necessary for the research activity (s 27(1)(d));
- information about a person's inherited characteristics must be necessary for the research activity (s 32(5)); and
- biometric information about a person must be necessary for the research activity (s 27(1)(d)).

[185] Paragraph 2.3.7

In effect, the Act outlines and requires the usual requirements for ethical and responsible informed consent procedures. The provisions underpin the importance of comprehensive SOPs and rigorous adherence to them. It should be remembered that research records including informed consent documentation may be solicited by interested parties via applications in terms of the Promotion of Access to Information Act 2 of 2000.'[186]

It is evident from the extracts cited above that information security was the focus when the guideline was revised. However, it is crucial that all provisions of the POPIA should be applied to research which includes identifiable personal information.

Research data management and research ethics approval (which is usually where consents are reviewed) are well-established policy areas with established structures (e.g. RECs) within public universities. The POPIA will not necessitate a wholesale overhaul of these policies and structures but requires some adjustments and the effective implementation of existing policies.

All universities must:

- have a research data management policy and procedure, which must include the requirements for a research data management plan and valid research consents;
- develop a privacy impact assessment to identify research projects which have critical privacy implications for research participants;
- ensure that both the research data management policy and privacy impact assessment are implemented via existing research ethics approval processes;
- ensure that all principal investigators complete certified training in research data management and privacy; and
- ensure that other researchers complete awareness training in research data management and privacy.

20. DIRECT MARKETING AND DONATIONS

Universities usually send direct marketing to prospective students, to registered students, and to alumni. The POPIA makes fairly significant changes to the legal framework within which direct marketing must be conducted.

Most complaints received by Information Regulator

It is important to note that most of the complaints received by the Information Regulator relates to unsolicited 'direct marketing'.

20.1. What is direct marketing?

20.1.1. Forms of direct marketing governed by the POPIA

[186] Paragraph 3.1.8.

Relevant sections:

- The definition of 'direct marketing'
- The definition of 'electronic communication'
- Section 69(1) (Direct marketing by means of unsolicited electronic communication)

The definition of direct marketing in the POPIA contains the following elements:

- the communication must be directed at an identified or identifiable data subject or group of data subjects;
- the communication must be in the form of an 'electronic communication'; and
- the communication must have the direct or indirect purpose of promoting a business or goods or services or to request donations.

In this section each of these elements will be discussed.

20.1.1.1. Directed at an identified or identifiable data subject or group of data subjects

For a communication to qualify as direct marketing it must be directed at an identified or identifiable data subject or group of data subjects.[187] When a responsible party is in possession of a data subject's contact details, marketing transmitted to those contact details will be considered 'direct marketing' as the marketer is targeting that data subject.

Direct marketing can also be transmitted via social media platforms to 'custom audiences'. When targeting a custom audience, a marketer typically provides the social media platform with contact details in its database which the social media platform then matches with users who are then specifically targeted.

The following is not direct marketing:

- indiscriminate or blanket marketing (e.g. adverts shown to all visitors to a website);[188] and
- if the communication is directed at a group of people who share certain attributes (e.g. females in Cape Town over the age of 35), it is not direct marketing as the institution cannot identify the individuals who will receive it.

[187] The definition of 'direct marketing' in section 1 of the POPIA.
[188] Information Commissioner's Office *Direct marketing* 14.

20.1.1.2. The communication must be in the form of an 'electronic communication'

The definition of 'direct marketing' in section 1 refers to marketing done in person, by mail, or by 'electronic communication'.[189] While the other provisions of the POPIA will apply to all forms of direct marketing, section 69 that regulates when consent is required, only applies to 'electronic communications'.

The POPIA defines 'electronic communication' as messages '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'.

Electronic communication includes:

- email
- SMS
- fax
- automatic calling machines[190]
- direct messaging via social media;[191] and
- advertising through social media platforms or display banners when a custom audience is targeted.

The following types of communication will not be subject to section 69 of the POPIA:

- approaching a data subject in person;
- telemarketing (unless it is made by automatic calling machines[192] or the telemarketer leaves a voice message); and
- mail.

Even though section 69 does not apply to these forms of communication, the rest of the POPIA is still applicable. For instance, the direct marketing activity will still have to be justified in terms of section 11[193] and the POPIA will

[189] The definition of 'direct marketing' in section 1 of the POPIA.
[190] Section 69(1).
[191] Information Commissioner's Office Guide to the Privacy and Electronic Communication Regulation 22.
[192] Section 69(1).
[193] This is discussed in part C, section 3.

determine whether the personal information used in the direct marketing was collected from a lawful source.[194]

Direct marketing by approaching a data subject in person, by telephone, or mail is also regulated by the Consumer Protection Act (the CPA).[195] Section 11 of the CPA provides that direct marketing can be sent unless the consumer has pre-emptively blocked direct marketing or unsubscribes.

20.1.1.3. For the direct or indirect purpose of promoting an institution or goods or services or to request donations

Certain communication will not constitute direct marketing, this includes communication that is:

- used to conduct genuine market research;[196]
- required to be sent by law; or
- required for the conclusion or performance of a contract.

Institutions must categorise communication into mandatory and optional messages. It is not advisable to send both mandatory and optional messages in one message as the data subject is then deprived of the opportunity to unsubscribe from the optional message. Or worse yet, in an attempt to opt out of the direct marketing, the data subject also now no longer receives important information.

Communication sent for the purpose of asking for a donation is also considered direct marketing. Institutions in this Industry often approach alumni to solicit donations.

20.2. Consent for direct marketing

Relevant section:

Section 69(1) (Direct marketing by means of unsolicited electronic communication)

The POPIA states that to send direct marketing, an institution must obtain the data subjects consent.[197] To decide whether consent is required, it is important to distinguish between instances where the marketers approached the recipient and instances where the recipient solicited the marketing from the marketer.

20.2.1. When the recipient solicited the marketing

[194] This is discussed in part C, section 8.
[195] Act 68 of 2008.
[196] Information Commissioner's Office *Direct marketing* 14. An institution cannot avoid direct marketing rules by labeling its message a survey or market research.
[197] Section 69(1)(a).

An opt-in consent is not required if:[198]

- the recipient contacts the marketer to enquire about or purchase goods or services;
- the recipient is told that the recipient's personal information would be used to send marketing communications;
- the marketer only sends marketing communication for its own goods or services, and those goods or services are similar to the ones the recipient contacted the marketer about or purchased;
- the recipient is given an opportunity to unsubscribe at the time the personal information was collected (i.e. the recipient was given an opportunity to opt out); and
- the recipient can unsubscribe every time the recipient receives marketing communications.

An opt-in is also not required if institutions can ensure that they:

- can prove when and where they obtained the information and whether it was in the context of the sale of a product or a service;
- only sent direct marketing for the same or similar products or services;
- can prove that they gave the data subject the opportunity to unsubscribe at collection; and
- always gave the data subject an opportunity to unsubscribe in subsequent communications.

If the institution cannot satisfy these requirements, they must request consent from their existing database.

20.2.2. Consent to send unsolicited direct marketing

An institution cannot send unsolicited direct marketing without data subjects' consent.[199] The POPIA states that if data subjects have previously declined to give consent to receive direct marketing, they may not be approached again. [200]

The consent obtained from the data subject must be valid in order for the direct marketing to be lawful. See the discussion on obtaining a valid consent in section 3.6.

[198] Section 69(3).
[199] Section 69(1)(a)
[200] Section 69(2)(a)(ii).

In addition, the Regulator has included a prescribed form for consent in its final Regulations.[201] The consent must be 'substantially similar' to the prescribed form.[202]

20.2.3. Third-party consents

Example

A university may ask for consent from a prospective student to send the student direct marketing. The student may also consent to receiving marketing from financial institutions that provide funding opportunities. The university may then pass on the student's information to the financial institution for the purposes of direct marketing to the student.

A third-party consent is when data subjects inform one institution that they consent to receiving marketing from another institution.[203] It is important to ensure that the consent the data subjects give to the third party is valid (See discussion on consent at 3.6). The consent must always be a positive choice that requires the data subject to actively do something to give consent.

Data subjects must have anticipated that their information would be passed on for their consent to be valid, and the consents cannot be blanket consents either.[204] When an institution gives information to a third party that institution must ensure that the consent state each third party that the information will be shared with.[205]

20.2.4. Unsubscribe

Data subjects must always be given an opportunity to object to receiving direct marketing communication from an institution. This opportunity to object must be free, and in an easy manner.[206] This opportunity must also be available to the data subject every time the institution sends out communication and if the data subject has not initially refused such use.[207]

The POPIA states that any direct marketing communication must contain an address or other contact details to which the data subject may send a request that such communication must stop.[208] If the data subjects had opted-out of communication, the institution can send them an immediate reply confirming that they have been unsubscribed.[209]

When a data subject objects to receiving direct marketing, an institution must ensure to add that data subject to a 'do not contact' list.[210] To ensure that you do not contact that data subject again, it is important to screen all marketing against this list.[211] It is

201 See Form 4.
202 See the definition of 'forms' in section 1 of the final Regulations.
203 Information Commissioner's Office *Direct marketing* 29.
204 Information Commissioner's Office *Direct marketing* 30.
205 Information Commissioner's Office *Direct marketing* 30.
206 Section 69(3)(c).
207 Section 69(3)(c)(ii).
208 Section 69(4)(b).
209 Information Commissioner's Office Guide to the Privacy and Electronic Communication Regulations 26.
210 Information Commissioner's Office Guide to the Privacy and Electronic Communication Regulations 26.
211 Information Commissioner's Office Guide to the Privacy and Electronic Communication Regulations 26.

important not to delete the data subjects' details in its entirety.[212] The reason for this is so that the institution can ensure that data subjects are not put back on a marketing list and contacted without their authorisation.[213]

20.3. Documenting processing for purposes of direct marketing

The POPIA requires that all processing activities are documented.[214] For the purposes of direct marketing this requirement is particularly important. This is because if a data subject withdraws consent to receive direct marketing, that data subject should not be contacted again for this purpose. As such the institution cannot automatically delete the data subject's information because should the data subject's information be erased, it will be impossible to determine, in future, whether the data subject has already withdrawn consent or not.

21. AUTOMATED DECISION-MAKING MUST FOLLOW SPECIFIC RULES

Relevant section:

Section 71 (Automated decision-making)

The POPIA prescribes specific rules for automated decision-making.[215]

Automated decision-making is:

- a decision that results in legal consequences for a data subject *or* that affects the data subject to a substantial degree; or
- a decision based on the automated processing of a profile of the data subject.

A profile can relate to the data subject's performance at work, credit worthiness, reliability, location, health, personal preferences, or personal conduct. This is also sometimes referred to as 'profiling'. A decision is considered automated when there is no human judgment involved.

Automated decision-making is only allowed if the legitimate interests of the data subjects have been protected.

Institutions should:

- implement a policy framework for the use of student personal information in automated decision-making that allocates specific responsibility for:
    - the collection of the personal information to be used;

[212] Information Commissioner's Office Guide to the Privacy and Electronic Communication Regulations 26.
[213] Information Commissioner's Office Guide to the Privacy and Electronic Communication Regulations 26.
[214] Section 17.
[215] Section 71.

- the anonymisation of the personal information where appropriate;
- the analytics processes to be performed on the personal information and the purpose of the processes;
- the decisions that will be taken based on the analysis (e.g. in learner analytics, who is responsible for the interventions); and
- the retention and custodianship of personal information used for and created during the automated decision-making.

- conduct a privacy impact assessment before automated decision-making processes are implemented. The process should include consultations with student representatives and key staff groups.
- ensure that algorithms used in automated decisions with serious consequences for data subjects are peer-reviewed to ensure that they are not only valid, but useful, fair and appropriate.
- ensure that they are transparent about automated decision-making and the algorithms that are going to be used.
- assess the quality of the personal information used in automated decision-making, particularly if the consequences of the decision are serious.
- provide all data subjects who are subjected to automated decision-making with meaningful access to the personal information used and created and the opportunity to make representations about the decision. There may be circumstances under which access could have a harmful impact on 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.
- ensure that inaccuracies in the information used in and created by automated decision-making can be 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.'
- ensure that all staff are trained and have a working understanding of legal, ethical, and unethical practice.

22. INFORMATION MATCHING PROGRAMMES

Relevant section:

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

- Section 40(1)*(b)*(ix)*(bb)* (Powers, duties and functions of Regulator)
- Section 44(2) (Regulator to have regard to certain matters)

An information matching programme involves the comparison of a record of the personal information about ten or more data subjects with another record containing the personal information of ten or more data subjects for the purpose of verifying information that may be used to take action with regard to an identifiable data subject.

The POPIA does not contain specific rules relating to information matching programmes. However, due to the fact that information matching programmes have the potential to invade the privacy of large numbers of data subjects, the POPIA states that codes of conduct must 'specify appropriate measures for information matching programmes'[216] and places additional duties on the Information Regulator to monitor legislation that makes provision for personal information in information matching programmes both in the public or the private sector.[217] The Information Regulator must have regard to the following issues when determining whether the information matching programme complies with the POPIA:[218]

- 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 the POPIA?
- Does the programme involve information matching at a scale that is excessive, having regard to the number of public or private bodies involved in the programme and the amount of detail about a data subject that will be matched.

Example

Public and private bodies in the higher education industry collect personal information relating to students to verify enrolment, academic results and qualifications, and transcripts.

If a university is considering taking part in an information matching programme it 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 all the principles of the POPIA;

[216] Section 60(4)*(a)*(i).
[217] Section 40(1)*(b)*(ix)*(bb)*.
[218] Section 44(2).

- taken steps to ensure that the public or private bodies who uses the information matching programme is doing so in a POPIA compliant manner;

- ensured that the algorithms used to match the information has been externally validated and reviewed 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 meaningful access to the personal information used and created the opportunity for 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), the information is not used in making a significant decision about the data subject before the data subject is informed of the negative result and given an opportunity to make representations.

D. COMPLIANCE STRUCTURES AND FRAMEWORKS

1. COMPLIANCE ROLES

In this section, the roles of Information Officers and Deputy Information Officers will be discussed.[219]

1.1. Information officer

The information officer of a public body is determined by the Promotion of Access to Information Act.

Relevant sections:

- The definition of 'information officer' in section 1 of the Promotion of Access to Information Act
- Section 55 (Duties and responsibilities of Information Officer)
- Section 4 of the final Regulations (Responsibilities of Information Officers)

In respect of a public body, the information officer will be the information officer of the public body as defined in section 1 of the Promotion of Access to Information Act. In respect of a public university this will be 'the chief executive officer, or equivalent officer.'

Information officers have the following responsibilities in terms of section 55 of the POPIA:

- ensuring compliance with the POPIA;
- dealing with requests made by data subjects and the Information Regulator; and
- working with the Information Regulator in relation to investigations.

The following responsibilities are listed in section 4 of the final Regulations:

- developing, implementing, monitoring and maintaining a compliance framework;
- conducting personal information impact assessments to ensure that adequate measures and standards exist in order to comply with the POPIA;
- developing, monitoring, and maintaining a manual as required by the Promotion of Access to Information Act;

[219] Section 1 and 56.

- developing internal measures and adequate systems to process requests for information about the processing of personal information or access to personal information; and
- conducting internal awareness sessions about POPIA compliance.

1.2. Deputy information officer

Relevant section:

Section 56 (Designation and delegation of deputy information officers)

Section 56 of the POPIA provides that public bodies must designate a deputy information officer(s) to perform the duties of the information officer. The appointment must be made in terms of section 17 of the Promotion of Access to Information Act.

2. COMPLIANCE FRAMEWORK

The Information Regulator has indicated that information officers must ensure that a 'compliance framework is developed, implemented, and monitored.' The POPIA does not stipulate what a compliance framework must contain. It should:

- define roles and responsibilities for POPIA compliance;
- set out the policies that will be created or amended;
- detail how the policies will be implemented;
- outline what training will be conducted; and
- determine how and how often compliance with POPIA will be monitored.

3. PERSONAL INFORMATION IMPACT ASSESSMENTS

In the final Regulation to the POPIA, the Information Regulator requires that personal information impact assessments must be done 'to ensure that adequate measures and standards exist to comply' with the POPIA.[220]

The objective of a personal information impact assessment is to 'systematically and comprehensively analyse' the processing of personal information in order to identify risks relating to personal information.[221] A personal information impact assessment should result in the following:

- a clear understanding of the risks associated with the particular processing activity;

[220] Regulation 4(1)*(c)*.
[221] Information Commissioner's Office Guide to the Privacy and Electronic Communication Regulation 192.

- agreed measures to reduce those risks; and
- documentary evidence that the process has taken place.[222]

END

Compiled by Universities SA (USAf)
Final version dated 24 June 2020 (Updated 1 September 2020)

Enqueries can be directed to Ms Jana van Wyk by email: jana@usaf.ac.za

[222] The Universities and Colleges Information Systems Association (UCISA) *Privacy Impact Assessment Toolkit* 6.