# Privacy and Information Protection Policy

| | | | | | |
|---|---|---|---|---|---|
| 1. | **Summary** | Policy for the implementation of Privacy and Data Protection in alignment with the POPI-A and moving towards Global best practise standards | | | |
| 2. | **Accountable Director(s):** | Barry Childs, Christoff Raath (Joint CEOs) | | | |
| 3. | **Applies to:** | All Insight policies and related procedural document | | | |
| 4. | **Groups/Individuals who have overseen the development of this policy:** | Faheem Suban, Barry Childs, Christoff Raath, Reinhild Nauhaus, Charmaine Roux, Masimba Mareverwa, Carol-Ann Lamberio, Andre Bellingham, Craig Getz | | | |
| 5. | **Groups/Individuals who have been consulted and have approved this policy:** | Faheem Suban | | | |
| 6. | **Ratifying committee and date of Final approval:** | Group Exco (Date) | | | |
| 7. | **Version:** | 1.0 | | | |
| 8. | **Available on:** | Intranet | X | Website | |
| 9. | **Related Documents:** | None. | | | |
| 10. | **Disseminated to:** | All employees and contractors of Insight | | | |
| 11. | **Date of Implementation:** | June 2020 | | | |
| 12. | **Date of next formal review:** | June 2021 | | | |

## Table of Contents

Revision History ..... 3
2. Introduction ..... 4
3. Policies Statement ..... 4
3.1. Objectives ..... 4
4. Scope of this policy ..... 4
5. Who this policy applies to ..... 4
5.1. Recommendations to contractors and third parties ..... 4
6. Definitions used in this policy ..... 5
7. Privacy Laws adherence ..... 7
8. Responsibilities and roles for Privacy ..... 7
9. Policy Framework ..... 8
9.1. Company overview ..... 9
9.2. Privacy Categories ..... 9
9.3. Principles and Conditions ..... 9
**9.3.1. Accountability ..... 9**
**9.3.2. Processing limitation ..... 10**
**9.3.3. Purpose Specification ..... 11**
**9.3.4. Further Processing limitation ..... 12**
**9.3.5. Information quality ..... 13**
**9.3.6. Openness, transparency, and notice ..... 13**
**9.3.7. Security Safeguards ..... 14**
**9.3.8. Data subject participation ..... 16**
**9.3.9. Third Party/Vendor Management ..... 18**
**9.3.10. Processing of personal information of children ..... 18**
**9.3.11. Free Flow of Information and Legitimate Cross-Border Restriction ..... 18**
**9.3.12. Response to requests and settlement of complaints ..... 19**
10. Training ..... 19
11. Dissemination and implementation ..... 20
12. Monitoring ..... 21
**12.1.1. Information asset register/data inventory ..... 22**



**12.1.2. Personal Information Management System (PIMS) ..... 23**

13. Review ..... 23

14. Appendix A – Applicable Republic Regulations ..... 23

14.1. The Constitution of the Republic of South Africa (1996) ..... 24

14.2. The Promotion of Access to Information Act (PAIA, 2000) ..... 24

14.3. The Electronic Communications Transmissions Act (ECTA, 2002) ..... 24

14.4. The Protection of Personal Information Act (POPI-A, 2013) ..... 25

14.5. Basic Conditions of Employment Act (1997) ..... 25

14.6. Labour relations act (LRA) ..... 26

14.7. UIF and SARS ..... 26

14.8. Employment Equity ..... 26

14.9. Skills development act (1998) ..... 27

14.10. Occupational Health and Safety Act ..... 27

15. Appendix B - Global privacy standards and best practice frameworks ..... 27

# Revision History

| Version | Person | Change Made |
|---|---|---|
| 1 | Kim Muller | Initial Version created with input from the IT Governance templates, COBIT 2019, POPI-A, PAIA Act, ECT Act and other applicable regulations (referred in Appendix A) and standards and frameworks (referred in Appendix B) |



# 2. Introduction

Insight Actuaries and Consultants (Insight) is a law-abiding consulting company domiciled in the Republic of South Africa. Insight is committed to good governance for long term sustainability and in balancing the interests of our all our stakeholders. This policy sets out our commitment to all our stakeholders to ensure their Right to Privacy and the information we process on their behalf is protected against unlawful collection, retention, dissemination and use.

# 3. Policies Statement

The Board of Directors and management of Insight Actuaries and Consultants located at Ground Floor, Block J, 400 15th Road, Central Park, Midrand are committed to compliance with all applicable South African laws and any additional regulations contractually agreed with our clients, in respect of personal information, and the protection of the "rights and freedoms" of persons whose information Insight collects and operates in accordance with the Protection of Personal Information (POPI) Act (2013).

## 3.1. Objectives

The objective of this Policy is to clearly define Insight's role and approach in terms of the protection of a person's right to Privacy in conformance with POPI-A as we progress towards applying International Privacy principles as the goal to be a globally respected and trusted operator.

# 4. Scope of this policy

The document focuses on the implementation of Privacy and Information Protection in Insight to ensure alignment from strategy to implementation and ongoing operations. The POPI-Aregulations and this policy apply to all of Insight's personal information processing functions.

Insight's objectives for Privacy and information protection are detailed in the Insight Privacy Objectives Record.

# 5. Who this policy applies to

All employees, contractors and data processing outsourced suppliers. Any breach of this policy, the Privacy Information Management System or POPI-A will be dealt with under the Insight disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

## 5.1. Recommendations to contractors and third parties

Partners and any third parties, working with or for Insight, and who have access to personal information, will be expected to have read, understood and to comply with this policy. No third party may access personal information held by Insight without having first entered into a data confidentiality agreement, which imposes on the third party, obligations no less onerous than those to which Insight is committed, and which gives Insight the right to audit compliance with the agreement.

# 6. Definitions used in this policy

The following definitions are noted from POPI-A and best practice frameworks used in this document:

- "**biometrics"** means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition
- "**child**" means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him or herself
- "**data**" means information in raw or unorganised form such as alphabets, numbers or symbols that refer to or represent, conditions, ideas, or objects. Data is limitless and present everywhere in the universe.
- A "**data subject**" is the person to whom the personal information relates;
- **"de-identify**", in relation to personal information of a data subject, means to delete any information that
    - Can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
    - Can be linked by a reasonably foreseeable method to other information that identifies the data subject,

  And de-identified has a corresponding meaning.
- **direct-marketing** means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of—
    - Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or
    - Requesting the data subject to make a donation of any kind for any reason
- **ECT-A** means the Electronic Communications and Transactions Act,2002 (Act no. 25 of 2002)
- **"electronic communication**" means any text, voice, sound, or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient"
- **"enforcement notice"** means a notice issued in terms of section 95 of POPI-A.
- "**Information**" means data that is accurate and timely, specific and organised for a purpose, presented within a context that gives it meaning and relevance, and can lead to an increase in understanding or a decrease in uncertainty. It is valuable as it can effect a behaviour, a decision or an outcome.
- **Information Officer** In the case of a public body means the Chief Executive Officer or equivalent officer of that public body who is acting as such
- **"knowledge"** means human faculty resulting from interpreted information, an understanding that germinates from a combination of data, information, experience, and human interpretation. In an organisation or group context, knowledge is the sum of what is known and resides in the intelligence and competence of the people
- An "**operator**" is the person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party
- **PAI-A** means the Promotion of Access to Information Act
- A **Person** refers to a natural or juristic person
- **personal Information** is 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, religion, conscience, belief, culture, language and birth of an individual;
(b) information relating to the education or the medical, financial, criminal or employment history of the person;
(c) any identifying number, symbol, e-mail 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 .

- "**POPI-A"** means the Protect of Personal Information Act, 2013 (ACT NO. 4 OF 2013)
- "**private body**" means –
    a. A natural person who carries or has carried out any trade business or profession, but only in such capacity;
    b. An existing juristic person but excludes a public body
- "**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
- "**professional legal advisor**" means any legally qualifies person, whether in private practise or not, who lawfully provides a client, at its request, with independent, confidential legal advice
- "**public body**" means any department of state or administration in the national or provincial sphere of government or any functionary or institution exercising a power or performing a duty in terms of any legislation;
- "**public record**" means a record that is accessible in the public domain and which is in the possession of or under the control of a public body whether or not it was created by that public body
- **"record**" means any recorded information regardless of form or medium
- The "**Regulator**" is the information regulator established in terms of section 39 of POPI-A; the Regulator is a juristic person, whose functions include monitoring and enforcing compliance by public and private bodies with the provisions of POPI-A.
- "re-identify" means to resurrect any information that has been de-identified that can be used by a reasonably foreseeable method to identify the data subject
- **"Republic**" means the Republic of South Africa
- A "**responsible party**" is the public or private body or person which, alone or in conjunction with others, determines the purpose of and means for processing personal information; this reference is akin to the "**controller**" as defined in the Privacy Shield Framework.
- "**special personal information**" as per POPI-A (26) means personal information concerning religious or philosophical beliefs, race and ethnic origin, trade union membership, political persuasion, health or sex life, biometric information of a data-subject; criminal behaviour of



a data-subject to the extent that such information relates to the alleged commission by a data subject of any offence or any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

- "**unique identifier**" means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

# 7. Privacy Laws adherence

As a law-abiding juristic person domiciled in the Republic, Insight will ensure compliance of the various laws with regard to Privacy as identified in the Insight Privacy Environment Context. Of the countries in which Insight's client's operate, the Republic is the only country that follows a comprehensive privacy approach and hence the POPI-A is of focus.

In addition to POPI-A, it is acknowledged that a number of Acts of the Republic described in (Appendix A **Error! Reference source not found.**) must also be taken into account with regard to the obligations of information records and privacy matters.

# 8. Responsibilities and roles for Privacy

Top management and all those in managerial or supervisory roles throughout Insight are responsible for developing and encouraging good information handling practices within Insight; responsibilities are set out in individual job descriptions.

All Employees are responsible for ensuring that any personal information that Insight holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by Insight to receive that information and has entered into a confidentiality agreement.

In terms of POPI-A (53) a duly appointed Information Officer is a member of the senior management team and is accountable to the Board of Directors of Insight for the management of personal information within Insight and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This officer will be registered as per POPI-A (55) as soon as the Republic's Regulator is ready.

Insight's Information Officer is responsible for:

- The development and implementation of Privacy as required by this policy
- security and risk management in relation to compliance with the policy
- encouraging compliance by Insight management and employees with the conditions for the lawful processing of personal information;
- dealing with requests made to Insight pursuant to the POPI-A;
- working with the Regulator in relation to investigations conducted pursuant to Chapter 6 in relation to Insight;
- otherwise ensuring compliance by Insight with the provisions of the POPI-A and other Privacy related acts



- Developing, implementing, monitoring and maintaining a compliance framework for Insight
- ensuring appropriate procedures and policies are in place to keep personal information accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors
- ensuring employees are fully aware of their obligations and trained to follow the privacy procedures and use the tools provided such as the Data Privacy Impact Assessment Tool
- ensuring information impact assessments are conducted to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;
- reviewing and keeping record of the Data Privacy Impact Assessment Tool data flows applicable to personal information
- developing, monitoring and maintaining a manual and ensuring it is available to regulators and as prescribed in POPI-A (14) and (51) and the Promotion of Access to Information Act 2000 (Act No 2 of 2000)
- developing Internal measures together with adequate systems to process requests for information or access thereto;
- conducting internal awareness sessions regarding the provisions of the POPI-A, regulations made in terms of the Act, codes of conduct, or information obtained from the Regulator and other Privacy sources and frameworks;
- ensuring all employees are trained in the importance of collecting accurate data and keeping it maintained
- ensuring that Insight does not collect information that is not strictly necessary for the purpose for which it is obtained
- ensuring the appropriate training levels for Privacy and Information protection throughout Insight;
- ensuring measures are implemented that consider the reliability of employees (such as references etc.);
- ensuring the inclusion of data protection in employment contracts;
- ensuring disciplinary action measures for data breaches;
- monitoring staff for compliance with relevant data protection standards
- on a regular basis, reviewing the data protection impact assessment procedure and data privacy impact assessment tool to ensure that collected data continues to be adequate, relevant, accurate, updated and not excessive and to minimise the amount of personal information stored.; and
- including any additional aspects with regard to Privacy as may be prescribed by the regulator(s) from time to time.

All Insight employees must ensure a data flow mapping is conducted by completing the Data Privacy Impact Assessment Tool and provided to the Insight Information Officer for review and record keeping.

# 9. Policy Framework



## 9.1. Company overview

In terms of the South African Protection of Personal Information Act (POPI-A), Insight is a private juristic person offering actuarial and Business Intelligence services as an "operator" to private juristic persons and public bodies across the African and Australasian continents.

Insight largely fulfils an "operator" role by analysing and reporting on data provided by our clients. who are usually the "responsible party" in terms of the "data subject". The majority of Insight's product offerings are based on analytics and research using a combination of de-identified data received from our clients, the responsible party in terms of the data subject, and available public data.

In terms of Employee personal information and any other collection directly from a data-subject, Insight will ensure that the conditions set out in Chapter 3 of the POPI-A and all the measures that give effect to such conditions, are observed with, at the time of the determination of the purpose and means of the processing, and during processing itself.

## 9.2. Privacy Categories

Insight is aware that Privacy has multiple, often overlapping, dimensions, namely:

- Privacy of person
- Privacy of behaviour and actions
- Privacy of communications
- Privacy of information
- Privacy of thoughts and feelings
- Privacy of location and territory

These dimensions will be considered in the ongoing considerations for a person's right to privacy as new technologies and risks emerge, even if legislation lags the curve.

## 9.3. Principles and Conditions

Insight as Responsible Party and Operator will ensure conditions of lawful processing that are within its control. These will include the conditions as defined in Chapter 3 of the POPI-A.

All processing of personal information will be conducted in accordance with Insight's Privacy and Information Protection principle conditions as set out in this section.

### 9.3.1. Accountability

Insight supports the identification of personal information within the enterprise and establish the risk associated with the storing and processing of the information.

Executives will communicate their support for ensuring privacy and information security to all impacted stakeholders.



Executives are committed to establishing the required roles and responsibilities and their training for effective privacy practices and implementing IT systems to support new or updated manual or computerized business processes, and launch of enterprise programs and operations involving personal information.

Insight and our associated data processors are accountable for appropriate governance and risk management of personal information for which we have responsibility and ensuring associated activities are compliant with all associated legal requirements.

Privacy stakeholders, the applicable legal requirements and privacy frameworks have been identified and implemented to support risk mitigation and legal compliance. Privacy risk will be analysed and assessed throughout the enterprise. Roles, responsibility, accountability and authority for performing privacy risk management processes will be assigned and monitored.

In addition, Insight will document, communicate, assign and maintain appropriate Privacy and Information protection policies and supporting procedures and standards.

Personal information will be Identified, inventoried and managed.

Where Insight is the Responsible Party, Insight will comply with the conditions set out in POPI-A as well as the measures that give effect to such conditions.

Conditions will be complied with both during the initial determination of the purpose and means of the processing as well as during the processing itself.

Where Insight assumes an operator role, contracts put in place with the responsible parties will ensure Insight provides the same level of protection as the responsible party

Insight is committed to adhere to codes of conduct, implement technical and organisational measures, as well as adopt techniques such as Privacy and Information protection by design, data protection impact assessments, breach notification procedures and incident response plans.

### 9.3.2. Processing limitation

The Insight data inventory will record all issues and limitations regarding data accuracy and steps taken to rectify.

Where Insight may have passed inaccurate or out-of-date information to third-party organisations, Insight will make appropriate arrangements to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal information to the third party where this is required.

When processing information Insight will ensure the relevant consent was provided by the data-subject and responsible party and cease processing as soon as is reasonably possible when a consent withdrawal is received.

Personal Information will be processed:

- in a lawful and reasonable manner for which consent was granted
- only for the original agreed purpose specified and explicitly defined

- in a manner that is adequate, relevant, and not excessive, protects the legitimate interest of the data subject or responsible party, does not infringe their privacy, or as required by law

Insight will obtain implicit or explicit consent prior to

- commencing collection activities, as appropriate and according to what the corresponding regulation mandates for the associated situation, with respect to the collection, use and disclosure of personal information.
- using the personal information for other purposes beyond those for which the personal information was originally collected
- the transfer of personal information to third parties and other jurisdictions

All Personal information under Insight's control will:

- be retained as per Insight's Retention of Records Procedure, and in line with any statutory obligations, not be stored for periods longer that required
- once its retention date is passed, it will be securely deleted as per the Insight Security and Privacy policy and the Secure Disposal Procedure and Storage Media Procedure
- on an annual basis, the information officer will review the data inventory and validate any data that has expired and not yet deleted and take appropriate action
- any data retention that exceeds the retention periods defined in the procedure must be given written approval and signed off by the Information Officer with corresponding justification
- any personal information that is retained beyond the processing date, must be encrypted in order to protect the identity of the data subject in the event of a data breach as per the Insight Security and Privacy Policy.

In addition, Insight will:

- ensure that any notification received regarding change of circumstances is recorded and acted upon.
- Ensure personal information is not kept in a form that permits identification of data subjects for longer than is necessary and in relation to the purpose(s) for which the data was originally collected
- Implement appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject where personal information is to be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

### 9.3.3. Purpose Specification

Personal Information will be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party.

Steps will be taken in terms of POPI-A18(1) to ensure that the data subject is aware of the purpose of the collection of the information unless required by law.



The Insight Privacy Procedure sets out the relevant procedures for ensuring data obtained is limited to the specified purposes. Evidence of procedures followed are recorded in the Insight Privacy Register of processing including any deviations and notifications reported to the Registrar.

As per the defined procedure, Insight's Information Officer is responsible for ensuring that Insight does not collect information that is not strictly necessary for the purpose for which it is obtained (refer to the Insight Data Privacy Impact Assessment Tool for the data flow/mapping).

All data collection forms (electronic or paper-based), including data collection requirements in new information systems, will include a fair processing statement or link to the Insight privacy statement and be approved by the Information Officer. It is also the responsibility of the data subject to ensure that data held by Insight is accurate and up to date. Completion of a registration or application form by a data subject must include a statement that the data contained therein is accurate at the date of submission and that they are required to notify Insight of any changes in circumstance to enable personal records to be updated accordingly. Instructions for updating records must be made available.

The Information Officer will ensure that, on an annual basis, the data protection impact assessment procedure and data privacy impact assessment tool are reviewed to ensure that collected data continues to be adequate, relevant, accurate, updated and not excessive and to minimise the amount of personal information stored. Every effort will be made to rectify inaccurate data or erase data no longer required.

As a data provider, Insight will ensure that Personal information that is used on an ongoing basis, including information that is disclosed to third parties, will generally be accurate, compete and up to date to the extent necessary

- for the purposes of use; and
- to minimize the possibility that inappropriate or inaccurate information may be used to make a decision about the data subject.

Insight will not update personal information unless such a process is necessary to fulfil the purposes for which the information was collected.

Records of Personal Information will not be retained by Insight longer than is necessary for achieving the purpose for which the information was collected or subsequently processed unless required by law.

### 9.3.4. Further Processing limitation

Further processing of personal information will be in accordance or compatible for the purpose for which it was collected.

Insight will assess whether the further processing is compatible with the purpose of collection as set out in the Insight Privacy Procedure and applying the data privacy impact assessment tool, taking into consideration:

- The relationship between the purpose of the intended further processing and the purpose for which the information has been collected



- The nature of the information concerned
- The consequences of the intended further processing for the data subject
- The manner in which the information has been collected;
- Any contractual rights and obligations between Insight and the other contracted parties and data subjects; and
- Further processing required by law

Evidence of procedures followed are recorded in the Insight Privacy Register of processing including any deviations and notifications reported to the Registrar.

### 9.3.5. Information quality

Where Insight is the responsible party, Insight will take necessary steps to ensure that personal information is complete, accurate, not misleading and updated where necessary taking into account the purpose for which it is being processed and will be further processed.

### 9.3.6. Openness, transparency, and notice

Insight will maintain the documentation of all its processing operations as required by POPI-A (14) (51).

Insight's Privacy Notice Procedure is set out in the Insight Privacy Notice. Privacy Notices issued, conditions for processing and withdrawals are recorded in Insight's Privacy Notice Register which is open for inspection by the Registrar and impacted parties.

Insight will continue to make efforts to ensure its Privacy Notices are understandable and accessible and communication with data subject's is in an intelligible form using clear and plain language.
Where Insight is the responsible party, data subjects will be provided:

- Insight's name, address
- the contact details of the Information Officer.

When collecting and using personal information where the data-subject will be identifiable, Insight will:

1. describe and specify the purpose(s) for which personal information is collected in the privacy notice or other means of communication, when the request for personal information is made, ensuring that the choices available to the data subject are understood (e.g., for accessing, updating, restricting access to their associated personal information)
2. describe the laws authorising or requiring the information;
3. advise whether the collection is voluntary or mandatory;
4. advise the consequences of failure to provide the information;
5. advise on any intention to transfer the information to a third country or International organisation and the level of protection afforded to the information by that third country of international organisation;
6. align the subsequent uses of the personal information with the purpose(s) provided, as well as with the consents obtained, and be in compliance with, associated legal requirements for use limitation.

7. Communicate when necessary with the Registrar about issues regarding legitimate purposes and use limitations.

On request, Insight will provide the following information to data subjects:

- Clear and easily accessible information about its privacy management program, policies and practices. Such practices will also be provided to whoever requests such information to support transparency and legitimacy.
- Insight's privacy notice and accurate details about:
  - the personal information that is being collected, derived and processed
  - the purpose(s) for these actions.
  - to whom and to which jurisdiction the personal information might be disclosed or transferred.
  - the identity of the responsible party including information on how to contact the responsible party.
  - whether the source was obtained from the data subject(s) or from other sources.

### 9.3.7. Security Safeguards

Insight will secure the integrity and confidentiality of all personal information in its possession or under its control and put the appropriate security safeguards in place to ensure that any personal information held is kept securely and is not, under any conditions, disclosed to any third party unless that third party has been specifically authorised by the responsible party to receive that information and has entered into an agreement to ensure confidentiality.

Insight will identify and assess all reasonably foreseeable internal and external risks to personal information in its possession or under its control. During the assessment, the extent of the possible damage or loss that might be caused to persons, as well as to Insight's reputation and trust relationships, must be considered should a breach occur to inform the controls required in alignment with the existing information security policies and applicable laws and regulations that Insight has already implemented.

Reasonable technical and organisational measures will be taken to prevent unauthorised access, processing, loss, damage, or destruction of personal information.

As a responsible party Insight will:

- establish and maintain appropriate security safeguards as reasonably required
- regularly verify safeguards to ensure they are effectively implemented
- continually update in response to new risks or deficiencies in previously implemented safeguards
- notify the Regulator; where applicable the data subject (where they can be identified and not under criminal suspicion as per POPI-A (22-3)(4)(5); of any personal information under Insight's control that is reasonably believed to have be accessed or acquired by unauthorised persons as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of Insight's information

system as per the Insight Incident response procedure. ; if requested by the regulator, publish in the compromise in the specified manner.

As an operator, Insight will agree contractual requirements and obligations required by the responsible party for alignment of risk identification methods and security controls and procedures as required by POPI-A (20) (21). Insight will notify the responsible party immediately where there are reasonable grounds to believe that any personal information provided by the responsible party to Insight has been accessed or acquired by any unauthorised person.

All personal information will be made accessible only to those who need to use it, and access may only be granted in line with the Insight Access Control Policy. All personal information will be treated with the highest security and must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected in line with corporate requirements in the Insight Access Control Policy; and/or
- stored on (removable) computer media which are encrypted in line with Secure Disposal of Storage Media.

Care must be taken to ensure that PC screens and terminals are not visible except to authorised employees of Insight. Employees are required to enter into an Acceptable Use Agreement before they are given access to organisational information of any sort, which details rules on screen time-outs.

Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit written authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving in line with the Insight Security and Privacy Policy.

Personal information may only be deleted or disposed of in line with the Insight Retention of Records Procedure. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs on which personal information were stored are to be removed and immediately destroyed before disposal.

Processing of personal information 'off-site' presents a potentially greater risk of loss, theft or damage. Staff must be specifically authorised to process data off-site.

Insight will establish security safeguards that include administrative, technical and physical security controls and that address confidentiality, integrity and availability of information in all forms, to mitigate risk to appropriate levels. To the end, Insight will consider putting in place a number of technical measures, as appropriate, such as:

- physical access controls to electronic and paper based records;
- a clear desk policy and drive its adoption;
- storing of paper-based data in lockable fire-proof cabinets;
- restrictions for the use of portable electronic devices outside of the workplace;
- restrictions for the use of employee's own personal device being used in the workplace
- password protection and associated clear rules;
- regular backups of personal information and storing the media off-site;



- Automatic locking of idle terminals
- Removal of access rights for USB and other memory media
- Virus checking software and firewalls
- Role-based access rights including those assigned to temporary staff
- Encryption of devices that leave the organisations premises such as laptops
- Security of local and wide area networks
- Privacy enhancing technologies such as pseudonymisation and anonymisation;
- Identifying appropriate international security standards relevant to Insight
- the imposition of contractual obligations to take appropriate security measures when transferring data outside of the Republic.

Insight will establish methods to prevent, identify quickly, respond to and effectively mitigate privacy breaches. Insight shall:

- Establish a documented policy and supporting procedure for identifying, escalating and reporting incidents of personal information breaches to data subjects and relevant data protection authorities, as necessary, in a timely manner, to mitigate potential legal and reputational risk.
- Maintain records of all personal information breaches including incident details, actions and progress with investigation, remediation and monitoring the progress until the incident is closed.
- Implement remediation actions to prevent reoccurrence of personal information breaches of a similar nature.

### 9.3.8. Data subject participation

Insight acknowledges the rights of Data-subjects and will ensure they may exercise their rights:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about the mechanics of automated decision-taking process that will significantly affect them.
- To not have significant decisions that will affect them taken solely by automated process.
- To take action to rectify, block, erase (including the right to be forgotten), or destroy inaccurate data.
- To request the Regulator to assess whether any provision of the POPI-Aregulation has been contravened.
- To have personal information provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
- To object to any automated profiling that is occurring without consent.
- Insight ensures that data subjects may exercise these rights:

Having received adequate proof of identity, Insight will provide data subjects the following rights and capabilities:



- Confirm, free of charge, whether or not Insight holds personal information about the data subject.
- Provide the record of personal information about the data subject including a description of the personal information held and identity of all third parties, or categories of third parties, who have or have had access to the information in a reasonable manner, format and generally understandable form, within a reasonable time and at a prescribed fee if applicable.
- provide the data-subject in upfront and in writing, the applicable fees for services requested.
- access to their personal information in full or part for which Insight is legally obliged.
- provide lawful grounds for refusal of any access to records requested based on POPI-A (Ch4(2)); PAI-A (Ch4(3)(30)(61) in full or part.
- request the correction, deletion, destruction of personal information about the data-subject in Insight's possession or control that is inaccurate, misleading or obtained unlawfully or no Consent

To give effect to the data subject's rights, Insight will put in place:

- The Insight Access Request Procedure provides confirmation from Insight about whether Insight has personal information relating to the data subjects, and when, why and where the information was obtained.
- The Insight Access Request Procedure also provides data subjects with access, within a reasonable time and at a reasonable cost, if applicable, to their associated personal information, in an easy to understand format. Any associated charges should not be excessive beyond that which the associated data protection authority would consider to be appropriate.
- The identity of the individual is validated prior to Insight providing the appropriate information to fulfil the data subject's request.
- The Insight Complaints Procedure provides the data subject with the opportunity to challenge the accuracy or use of personal information relating to them and, if the challenge is successful, to have the personal information erased, rectified, completed or amended.
- The Insight Request portability procedure provides the data subject with portability of his or her associated personal information that can allow for the data subject to move the information to a different service provider.
- The Insight Consent Procedure provides the data subject the opportunity to provide consent/authorization, or deny the same, prior to the data controller continuing with the collection and use of personal information.
- The Insight Request Access Procedure enables the data subject to request an accounting of disclosures that details with whom, when, why and how personal information has been shared and gives the data subject the opportunity to request restriction of uses of personal information.
- Insight shall provide clearly communicated reasons why any data subject requests about personal information are denied, and the data subject will be given a process to challenge such denial.
- All requests for access to personal information can be directed as per the PAI-A (2000) in English to:
  Insight Information Officer
  Address: Ground Floor, Block J Central, Central Park, Midrand, 1682
  Email address : informationofficer@insight.co.za
  Telephone: +27 11 541 0900

Any requests made on behalf of a person, are required to submit proof of the capacity in which the requester is making the request.

An individual who because of illiteracy or a disability is unable to make a request for access to a record, may make an oral request and the information officer will reduce the oral request to writing in the prescribed form and provide a copy thereof to the requester.

The POPI-A forms are available here: POPI-A Forms Link.

### 9.3.9. Third Party/Vendor Management

Insight shall provide ongoing oversight of third parties to which Insight entrusts any type of access to the personal information for which Insight is responsible. Insight will:

- Implement governance and risk management processes and apply contractual, administrative and audit measures to ensure the appropriate protections and use of personal information that are transferred to, maintained, processed, controlled and/or accessible by all associated third parties
- Require all third parties with any type of access to personal information to report personal information breaches in a timely manner to Insight without delay as defined by Insight's contractual agreements and as required by any applicable data protection authorities.

Insight employees may not disclose personal information to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All employees should exercise caution when asked to disclose personal information held on another individual to a third party and will be required to attend specific training that enables them to deal effectively with any such risk. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of Insight's business.

All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Information Officer.

### 9.3.10. Processing of personal information of children

Insight currently only processes information as an operator for children under eighteen in a de-identified manner for research and reporting purposes that is in the legitimate interests of the responsible party

### 9.3.11. Free Flow of Information and Legitimate Cross-Border Restriction

As regulated by POPI-A (72), Insight will not transfer personal information about a data-subject to a third party who is in a foreign country unless the third party, who is the recipient of the information, is subject to a law binding corporate rules or binding agreement which provide an adequate level of protection that effectively upholds principles for reasonable processing of the information that are



substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural or juristic person.

Insight will ensure the level of security and privacy protections of the jurisdiction to which the information is transferred is at least equivalent to the protections within the Republic and meets the requirements of the Regulator, or that a contract signed between parties establishes such requirements.

The Insight Privacy Procedure includes the relevant procedures for cross border transfers and evidence is recorded in the Insight Privacy Register of processing including any deviations and notifications reported to the Registrar.

Insight's Information Officer is responsible for ensuring that the necessary authorisations are obtained from impacted parties and the Regulator if required, based on the risk impact for personal data moving across borders as per the Insight Data Privacy Impact Assessment Tool.

### 9.3.12. Response to requests and settlement of complaints

Insight's Information officer must respond to requests for rectification from data subjects within one month as per the Insight Access Request Procedure. This can be extended to a further two months for complex requests. If Insight decides not to comply with the request, the Information Officer must respond to the data subject to explain its reasoning and inform them of their right to complain to the Regulator.

If it appears from a complaint or any written reply to the complaint under the POPI-A or during a conciliation meeting, that it may be possible to secure a settlement between the parties and if appropriate, satisfactory assurances as contemplated in the Act, the Regulator may confer with the parties in person, by electronic communication means, or by any other means as is deemed appropriate to endeavour to obtain a settlement and if appropriate, satisfactory assurances as contemplated the Act.

If during the process the Regulator decides to convene a settlement meeting, the Regulator must, as soon as it is practically possible, inform the data subject and the responsible party on the relevant form of the date, time and place of the settlement meeting.

For the purpose of settlement proceedings, the Regulator has the same powers of a conciliator contemplated. The Regulator must issue a settlement certificate on Form 10 within a reasonable time after the date of the conclusion of the settlement meeting.

If no settlement and assurance is secured or if either or both of the parties did not wish to attend a settlement meeting, the Regulator must proceed with the matter as provided for in terms of section 76 of the Act.

# 10. Training

Periodic privacy training and ongoing awareness communications will be provided to existing and new employees and contractors. Training will be done at least annually or when a significant event or organizational change occurs, warranting an update.

Training and awareness activities will include role-based training, situational training and professional certifications for key workforce members based on their responsibilities and associated privacy risk.

Training and awareness communications will cover all internal privacy policies, and the enterprise privacy notices, communications with data subjects, and any other activity that involves personal information. Satisfactory privacy training completion will be tracked on the Insight Training Register and documentation retained for 3 years as required by legislation.

Executive Management must promote Privacy and Information protection training and awareness programmes and make resources available in order to raise awareness.

The Information Officer is responsible for ensuring:

- all Insight employees have a general knowledge of the Privacy laws and Insight's Privacy and Information Security policy.
- all employees are trained in the importance of collecting accurate data and maintaining it.
- employees with day-to-day responsibilities involving personal information and processing operations, and those with permanent/regular access to personal information, fully understand and demonstrate competence and compliance with this policy, the associated Privacy laws, as well as the required procedures and supporting systems.
- all employees are kept up to date and informed of any issues that arise related to personal information.
- a list of relevant external bodies is maintained, the most important of which is the Regulator of the Republic.
- the importance of information protection and the security requirements are demonstrated and communicated to employees
- employees understand how and why personal information is processed in accordance with Insight's policies and procedures
- employees are provided with specific training on any information security requirements and procedures applicable to information protection and the data processing within their individual day-to-day roles and responsibilities, including reporting personal information breaches.
- employees are provided with training on dealing with complaints relating to data protection and processing personal information.
- records are maintained of the relevant training undertaken by each person.
- All employees with day-to-day responsibilities involving personal information and processing operations will at planned intervals assess the PIMS and its capability to demonstrate compliance to POPI-A.

# 11. Dissemination and implementation

The following approach is recommended for the initial roll-out of the program:

1. Review, modify, approve, and publish the required Privacy and Information protection policies, procedures, tools and records, including with Insight's legal advisor.



2. Appoint the Information Officer.
3. Prioritise areas most likely to be storing and / or processing personal information.
4. Conduct initial training and awareness sessions with employees in the impacted areas.
5. Map out the information flows and establish areas where Personal Information is stored and processed.
6. Establish a security programme to implement effective controls for information protection in the required areas.
7. Review and update the policies, procedures and tools with feedback received from the pilot.
8. Prioritise areas for further roll out.
9. Continue with rollout and training until all employees in Insight have been trained and procedures operationalised.
10. Review and update as necessary third-party contracts.
11. Establish and rollout a communication programme for clients and discuss any contractual amendments and assistance required and alignment with their Privacy implementation.
12. Information officer to monitor, review and update policies, procedures, and tools.
13. Once the Regulator is established notify them of the appointed Information Officer.

# 12. Monitoring

The Information Officer is responsible for reviewing the register of processing annually in the light of any changes to Insight's activities (as determined by changes to the data inventory register and the management review) and to any additional requirements identified by means of data protection impact assessments. This register needs to be available on the supervisory authority's request.

Insight shall establish appropriate and consistent monitoring, measuring and reporting of the effectiveness of the privacy management program and tools and establish framework for measuring and monitoring the following

- Effectiveness of the privacy management program.
- Level of compliance with applicable policies, standards and legal requirements.
- Use and implementation of privacy tools.
- Types and numbers of privacy breaches that occur.
- Privacy risk areas within Insight.
- Third parties that have access to personal information and the associated risk levels
- Report compliance with privacy policies, applicable standards and laws to key stakeholders.
- Integrate internationally accepted privacy practices into business practices, such as those from International Organization for Standardization (ISO), the National Institute of Standards and Technology (NIST) and ISACA.
- Establish procedures that cover the use of personal information in investigating, monitoring, continuous auditing, analytics, etc. done by internal and/or external auditors.

- Anonymize data if the local/national law is not allowed to monitor pure personal information for fraud/crime prevention or other.

### 12.1.1. Information asset register/data inventory

Insight has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its Privacy compliance project. Insight's data inventory and data flow determine:

- business processes that use personal information.
- source of personal information.
- volume of data subjects.
- description of each item of personal information.
- processing activity.
- maintains the inventory of data categories of personal information processed.
- documents the purpose(s) for which each category of personal information is used.
- recipients, and potential recipients, of the personal information.
- the role of the Organisation Name throughout the data flow.
- key systems and repositories.
- any data transfers.
- all retention and disposal requirements.

1.1 Insight is aware of any risks associated with the processing of types of personal information.

1.1.1 Insight assesses the level of risk to individuals associated with the processing of their personal information. Insight Data protection impact assessments (DPIA) are carried out in relation to the processing of personal information by Insight, and in relation to processing undertaken by other organisations on behalf of Insight.

1.1.2 Insight will manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

1.1.3 Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Insight will, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal information. A single DPIA may address a set of similar processing operations that present similar high risks.

1.1.4 Where, as a result of a DPIA it is clear that Insight is about to commence processing of personal information that could cause damage and/or distress to the data subjects, the decision as to whether or not Insight may proceed must be escalated for review to the Information Officer.

1.1.5 The Information Officer will, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the CEOs.

1.1.6 Appropriate controls will be selected from *ISO 27001, ISO 27017, ISO 27018, COBIT etc., as appropriate]* and applied to reduce the level of risk associated



with processing individual data to an acceptable level, by reference to Insight's documented risk acceptance criteria and the requirements of the POPI-A or other applicable regulations.

### 12.1.2. Personal Information Management System (PIMS)

In compliance with the ISO/IEC 27001 standards, Insight's Board of Directors has approved and supported the development, implementation, maintenance and continual improvement of a documented personal information management system ('PIMS') for Insight. All Employees, and certain external parties, will receive appropriate training.

In determining its scope for compliance with International standards and POPI-A regulations and in line with Insight's Privacy approach, Insight considers:

- any external and internal issues that may affect its ability to achieve the intended outcomes of its Privacy Information Management System (PIMS);
- specific needs and expectations of interested parties that are relevant to the implementation of the PIMS;
- the organisational objectives and obligations;
- the organisations acceptable level of risk; and
- any applicable statutory, regulatory or contractual obligations.

The PIMS Scope Statement is documented here <document links to be added once uploaded to SharePoint>.

Insight's objectives for Privacy conformance with the POPI-A when approved

- are consistent with this policy
- are measurable
- take into account ISO 27700, 27701 and the results from risk assessments and risk treatments
- are monitored, communicated and updated as appropriate

Insight documents its objectives in the Privacy Objectives Record in order to achieve these objectives, Insight has determined:

- what will be done.
- what resources will be required.
- who will be responsible.
- when it will be completed.
- how the results will be evaluated.

## 13. Review

The Information Officer must ensure that this policy is reviewed, updated and tabled for ratification and approval by the Insight Board at least on an annual basis.

## 14. Appendix A – Applicable Republic Regulations

A detailed context of Privacy is provided the Insight Privacy Context document.



In terms of Privacy in South Africa, The Constitution is the supreme law (section 2), and the state is required to respect, protect, promote and fulfil the rights in the Bill of Rights (section 7(2)). It is binding on both state and non-state actors (section 8). All rights in the Bill of Rights can be limited by a law of general application, to the extent that the limitation is reasonable and justifiable in an open and democratic society (section 36). Certain statutes also compel organs of the state or other parties to protect private information obtained from the public, such as the National Health Act 61 of 2003; the National Credit Act 34 of 2005; the Consumer Protection Act 68 of 2008; the Electronic Communication and Transactions Act 25 of 2002; and the Promotion of Access to Information Act 2 of 2000.

## 14.1. The Constitution of the Republic of South Africa (1996)

The cornerstone of South Africa's democracy enshrining the rights of the people of South Africa affirming the democratic values of dignity, equality and freedom. In terms of people's right to Privacy, states that **everyone has the Right to Privacy**, which includes the Right not to have their person, home or property searched, their possessions seized or the Privacy of their communications infringed.

## 14.2. The Promotion of Access to Information Act (PAIA, 2000)

This Act ensures that people can exercise their constitutional right of **access to information** that is **required for** the exercise or **protection of any rights**, subject to justifiable limitations aimed at the reasonable protection of privacy, commercial confidentiality and good governance in a manner that balances that right with other rights.

## 14.3. The Electronic Communications Transmissions Act (ECTA, 2002)

The ECT act aims to provide a structure to define, develop, regulate and govern e-commerce in South Africa. It applies to any form of communication: e-mail, internet, SMS etc. It enables / gives legal definition to electronic documents and signatures (typed name at the end of your email; a scanned image of your hand written signature, a digital signature and an advanced electronic signature (AES).

The Act further requires suppliers of cryptography services register their names and addresses with the Department of Communications to allow SAPS and other investigative authorities as a means for the challenge against cyber crime.

The aspects to be aware of from the ECTA are:

- the facilitation and regulation of electronic communications and transactions.
- promotion of universal access to electronic communications and transactions



- as well as for human resource development in electronic transactions; to prevent abuse of information systems.

## 14.4. The Protection of Personal Information Act (POPI-A, 2013)

POPI-A recognises that:

- the Constitution of the Republic of South Africa, 1996, provides that everyone has the right to privacy which includes the right to protection against the unlawful collection, retention, dissemination and use of personal information; and
- the need for economic and social progress with the framework of the information society requires the removal of unnecessary impediments to the free flow of information, including Personal Information in harmony with International standards

POPI-A aims to promote the protection of personal information processed by public and private bodies; to introduce certain conditions to establish minimum requirements for the processing of personal information and provide for the establishment of an Information Regulator to exercise certain powers, duties and functions. In addition, the Act provides for the rights of Persons regarding unsolicited communications and automated decision making and aims to regulate the flow of information across the borders of the Republic of South Africa.

The purpose of the POPI-A is to ensure that all South African Institutions conduct themselves in a responsible manner when collecting, processing, storing, sharing and destroying another entity's personal information by holding them accountable should they abuse or compromise an individual or entities personal information in any way.

## 14.5. Basic Conditions of Employment Act (1997)

In terms of the Basic conditions of employment Act (1997), Section 31 : Keeping of records

31. ( 1 ) Every employer must keep a record containing at least the following information:
(a) The employee's name and occupation;
(b) the time worked by each employee;
c) the remuneration paid to each employee
(d) the date of birth of any employee under 18 years of age
(c) any other prescribed information

(2) A record in terms of subsection must be kept by the employer for a period of three years from the date of the last entry in the record

(3) No person may make a false entry in a record maintained in terms of subsection (1). (4)

In particular, an employer is also legally obliged retain particulars of



- The employee's job description;
  - The date on which employment commenced;
  - The hours of work;
  - Remuneration particulars;
  - Leave provisions; and
  - Notice period.

SARS requires the information is kept for 5 years after termination of employment.

The statutory provision does not apply to employees who work less than 24 hours a month for that employer or employs less than five people.

It is also advisable to cater for other particulars, among them the benefits to which the employee is entitled, copyright and patents, restraint of trade agreements and a wage and attendance register. The employer should retain the records in question for three years after termination of employment.

Schedule 2 of the BCEA specifies the penalties which may be imposed on an employer for failing to comply with the provisions of the BCEA. The fines range from R100 to R500 per employee.

## 14.6. Labour relations act (LRA)

The Labour Relations Act (LRA) provides that an employer is legally obliged to keep records in compliance with any applicable collective agreement or arbitration award and is obliged to retain such records in their original form or a reproduced form for three years from the date of the event or end of the period to which they relate. An employer must keep a record of the prescribed details of any strike, lock-out or protest action involving its employees. LRA regulations contain a prescribed form, which the employer is obliged to complete and submit a copy thereof to the Department of Labour.

## 14.7. UIF and SARS

The Unemployment Insurance Contributions Act, together with the Income Tax Act, obliges employers to retain records of remuneration paid, tax which has been deducted and unemployment insurance fund contributions and payments for each employee. The records must be maintained in such form, including any electronic form, as may be prescribed by the revenue authorities. These records should be kept for five years from the date of the last entry and must be available for inspection by the South African Revenue Service and Unemployment Insurance Fund officials. An employer who contravenes these statutory provisions will be guilty of an offence and liable on conviction to a fine, to imprisonment for not more than 12 months or both the fine and imprisonment.

## 14.8. Employment Equity

The Employment Equity Act (EEA) places a legal obligation on "designated employers" to retain records of its workforce, its employment equity plan and other records relevant to its compliance with the EEA. It is advisable to keep records of all interviews conducted with job applicants. In terms of the EEA, a job applicant may challenge a recruitment decision on the basis of unfair discrimination within six months of the recruitment decision, a period for which the employer should retain the relevant records.



### 14.9. Skills development act (1998)

Records to be maintained of learnership agreements, disputes, skills development plans and training records including financial spend per employee.

### 14.10. Occupational Health and Safety Act

Any records relating to the management of incidents relating to persons and the Health and safety committee recommendations record to employers in terms of subsection 1a and of any report made to an inspector in terms of subsection 1b including details of the health of any person. Section 12(2) notes that individual results of biological monitoring and medical surveillance relating to the work of an employee requires written consent of an employee to be made available to any person other than the inspector.

## 15. Appendix B - Global privacy standards and best practice frameworks

There are a number of good practise frameworks that Insight strives towards in order to provide a solid foundation for Privacy, namely:

- ISO/IEC 27002:2013. Information technology—Security techniques—Code of practice for information security management: Section 15 The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) jointly issued this international standard, which was last updated and published in 2013. This Security Compliance Standard is part of a growing family of ISO/IEC Information Security Management Systems (ISMS) standards. ISO/IEC 27002 provides a security framework. Section 15 covers compliance, including legal requirements; security policies, standards and technical compliance; and information systems audit considerations. While this standard is not specific to privacy, this standard is often used to support the security requirements found in multiple privacy laws, regulations and standards, and includes a component for meeting legal requirements.
- ISO/IEC 27701 Privacy Information Management System (PIMS) helps organisations reconcile privacy regulatory requirements. The standard outlines a comprehensive set of operational controls that can be mapped to various regulations. Once mapped, the PIMS operational controls are implemented by privacy professionals and audited by internal or third-party auditors resulting in a certification and comprehensive evidence of conformity. A PIMS certification could be taken as evidence of POPI-Acompliance not as official POPI-Acertification until regulatory decisions are finalised.



- ISO/IEC 29100: Information technology—Security techniques—Privacy framework. This international standard was published in December 2011 and provides a privacy framework that specifies common privacy terminology; defines the actors and their roles in processing personally identifiable information (PII); describes privacy safeguarding considerations; and provides references to known privacy principles for information technology.
  www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45123
- ISO/IEC 15944-8: Information technology—Business Operational View—Identification of privacy protection requirements as external constraints on business transactions Modelling business transactions using scenarios and scenario components is done by specifying the applicable constraints on the data content using explicitly stated rules. External constraints apply to most business transactions. This part of ISO/IEC describes the business semantic descriptive techniques that are needed to support privacy protection requirements when modelling business transactions using the external constraints of jurisdictional domains. It was published in April 2012.
  www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51544
- ISO/IEC 27018:2014 Information technology—Security techniques—Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors ISO/IEC 27018:2014 establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect personal information in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.
  In particular, ISO/IEC 27018:2014 specifies guidelines that are based on ISO/IEC 27002, taking into consideration the regulatory requirements for the protection of personal information that may be applicable within the context of the information security risk environment(s) of a provider of public cloud services.
  www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61498
- BS 10012:2009—Data protection. Specification for a personal information management system British Standard (BS) 10012 specifies the requirements for a personal information management system (PIMS), which provides an infrastructure for, among other things, maintaining and improving compliance with the UK Data Protection Act (DPA) 1998. Rather than prescribing exactly how operations should be run, BS 10012 provides the framework that enables effective management of personal information. It can be used by enterprises of any size and sector to create a tailored management system that includes procedures in areas such as training and awareness, risk assessment, data sharing, retention, disposal of data and disclosure to third parties.
- The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the “rights and freedoms” of natural persons (i.e. living individuals) and to ensure that



personal information is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

- COBIT 2019: An integrated Global Standard for integrating industry standards, guidelines, regulations and best practices.
- NIST: The National Institute of Standards and Technology at the US Department of Commerce have provided a Cybersecurity framework (CSF) as a first line of defense for managing Risk
- SANS: A trusted resource for Information security and Privacy training, cyber security certifications and research.
- IT Governance: A UK Based firm providing frameworks and tools for improving Cybersecurity and Privacy practices.

Guidance from these frameworks are selected and applied effectively to ensure an efficient yet effective base for Data Privacy.