Government Gazette
Staatskoerant

REPUBLIC OF SOUTH AFRICA
REPUBLIEK VAN SUID AFRIKA

Vol. 730 30 April April 2026 No. 54594

ISSN 1682-5845

9 771682 584003 54594

GOVERNMENT NOTICES • GOEWERMENTSKENNISGEWINGS

DEPARTMENT OF JUSTICE AND CONSTITUTIONAL DEVELOPMENT

NO. 7415 **30 April 2026**

INFORMATION REGULATOR (SOUTH AFRICA)
Ensuring protection of your personal information and effective access to information

Woodmead North Office Park, 54 Maxwell Drive, Woodmead
Johannesburg, 2191, Gauteng Province, South Africa
P.O Box 31533, Braamfontein, Johannesburg, 2017
Email: enquiries@inforegulator.org.za
Website: www.inforegulator.org.za
Toll Free: +27 80 001 7160

21 APRIL 2026

NOTICE IN TERMS OF SECTION 61(2) OF THE PROTECTION OF PERSONAL INFORMATION ACT NO 4 OF 2013 (POPIA) ABOUT THE OWN INITIATIVE CODE OF CONDUCT OF THE INFORMATION REGULATOR ON THE PROCESSING OF PERSONAL INFORMATION AT GATED ACCESSES IN SOUTH AFRICA, ISSUED UNDER SECTION 60(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 (POPIA).

1. In terms of the provisions of section 61(2) of POPIA, the Information Regulator (Regulator) gives notice of the proposed *Own Initiative Code of Conduct on the Processing of Personal Information at Gated Accesses in South Africa* that deals with how personal information will be processed in the gated accesses.

2. The purpose of the code of conduct is to-
   2.1 to prescribe sector specific obligations that give practical effect to the eight conditions for lawful processing under POPIA in gated access environments
   2.2 and promote appropriate practices by all gated accesses in governing the processing of personal information in terms of POPIA; to ensure proportionality between security needs and privacy rights; standardise lawful access control practices; regulate high risk technologies (including CCTV and biometric systems); strengthen governance and accountability; and provide effective complaints and enforcement mechanisms.

3. The code of conduct scope-

3.1 This Code applies to any public or private body that determines the purpose and means of processing personal information at a gated accesses where appropriate, the processing of personal information (including personal information of data subjects).
and

3.2 the enforcement by gated accesses of the provisions of the code of conduct.

4. A notice will be published in the Government Gazette in compliance with section 61(2) of POPIA. Affected persons are invited to submit written comments to the Regulator email address: POPIACompliance@inforegulator.org.za. within fourteen (14) days after publication of the notice in the Government Gazette. A copy of the code of conduct will be made available on the Regulator's website, alternatively, a request for a copy of the code may be made by addressing correspondence to email address: POPIACompliance@inforegulator.org.za

Own Initiative Code of Conduct of the Information Regulator

On the processing of personal information at gated accesses in South Africa.

Issued under section 60(1) of the Protection of Personal Information Act 4 of 2013 (POPIA).

2025-26

INFORMATION REGULATOR
(SOUTH AFRICA)
Ensuring protection of your personal information and effective access to information

www.inforegulator.org.za

TABLE OF CONTENTS

Definitions.

"Access Control"	means "a set of rules and procedures implemented to provide for the identification of users, the granting and denying of access, the recording of access attempts, and the administrative tools necessary to manage and monitor access activities. [1]
"Body corporate"	means an entity established when the owners of units in a scheme, including the developer and any person who subsequently becomes an owner of a unit in that scheme, become members of the body corporate in terms of Section 2(1) of the Sectional Titles Schemes Management Act 8 of 2011.
"**CCTV**"	means "self-contained surveillance system comprising cameras, recorders and displays for monitoring activities and uses cables between the camera and the monitor".[2]
Compliance Framework	means "all of the interrelated and/or interacting components within an organisation that: • Sets out the organisation's approach to the management of all categories of compliance risk. The framework addresses aspects such as compliance strategy, objectives, governance, policy, roles and responsibilities, compliance risk appetite, process and techniques and reporting. • Establish and maintain (or contribute to, support, facilitate or enable establishing and maintaining) compliance related objectives and the activities, policies, procedures, processes and practices to achieve those objectives; and • Direct, guide, contribute to, facilitate, enable or support compliance related practices and activities."[3]
"Gated access''	means restricted entry to a specific area, requiring authorisation or credentials for access.[4] In the context of this Code of conduct, gated access includes access control by means of CCTV, physical guards,

1 Department of Public Service Commission; Access Management Sub-Guideline

2 By-Law No. 9 South African Intruder Detection Services Association Requirements for the Installation of a Video Surveillance System (VSS) Version 1.3– November 2024 SAIDSA

3 Generally Accepted Compliance Principles Framework, Compliance Institute of South Africa 2024, page 4

4 https://www.google.com/search?q=gated+access+meaning&sca

	and or other electronic features through which the personal information of data subjects is collected (for security purposes or other reasons) to control or restrict entrance to premises that are under the control of a public or private body (responsible party).
"Personal Information Impact Assessment"	means a systematic assessment of the processing that identifies the impact of risk that the process might have on the privacy of data subjects, and sets out recommendations for managing, minimising or eliminating that impact of risk.[5]
"Physical access control system"	means a system that allows organisations to not only enable access at premises with guarded or controlled accesses.[6] at residential communities, commercial/ corporate or public (government) buildings.
"Premises"	means a house or building, together with its land and outbuildings, occupied by residents, business or considered in an official context, such as residential estate or commercial / complex/office park etc.
"Profiling"	means a procedure which may involve a series of statistical deductions. It is often used to make predictions about people, using data from various sources to infer something about an individual, based on the qualities of others who appear statistically similar.[7]
"Regulator"	means the Information Regulator established in terms of Section 39 of POPIA.
"Regulations"	means Regulations made in terms of Section 112(2) of POPIA;
"Relevant body/bodies"	means any specified body or class of bodies, or any specified industry, profession, or vocation or class of industries, professions, or vocations that in the opinion of the Regulator which has sufficient representation; in the context of this Code specified body or class of bodies, include(s) body corporates, trustees, homeowners' associations, executive estate managers in the commercial/private and public sector etc.
"Relevant stakeholders"	means stakeholders, affected stakeholders or a body representing such stakeholders in terms of the *Guidelines to Develop Codes of Conduct issued by the Information Regulator.*

5 Guide to undertaking privacy impact assessments. May 2020 oaic.gov.au at 2. PIIA is not defined in POPIA, and the definition has been adapted.

6 https://www.entrust.com/resources/learn/what-is-physical-access-control-system 05.06.2025

7 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 at 7

	In the context of this Code, includes responsible parties in control of gated accesses and data subjects affected by processing at gated accesses.
‘‘Responsible party’’	means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information
“Trustees”	Trustees mean trustees of the body corporate who perform and exercise functions and powers of the body corporate subject to the provisions of the sectional titles’ schemes act, the rules and any restriction imposed, or direction given at a general meeting of the owners of sections.[8]

[8] Section 7 of the Sectional Titles Schemes Management Act, 8 of 2011. (STSMA)

1. INTRODUCTION

1.1. The preamble to the Protection of Personal Information Act 4 of 2013 (POPIA) recognises "the right to privacy", including protection against unlawful collection, retention, dissemination and use of personal information".

1.2. The Information Regulator (Regulator) is established in terms of section 39 of POPIA, as a juristic person and is mandated, in terms of section 40(1)(b), to monitor and enforce compliance by public and private bodies with the provisions of POPIA.

1.3. The Regulator is further empowered in terms of section 61(1) (a) of POPIA to issue a Code of Conduct on its own initiative. This Code is accordingly developed by the Regulator in terms of 61(1) (a) and regulates the processing of personal information of data subjects at the gated access entry points.

1.4. The Regulator shall use this Code following consultation with affected stakeholders, or with a body or bodies representing such stakeholders, in accordance with the provisions of POPIA.

1.5. Upon approval, this Code shall be binding on all responsible parties engaged in the processing of personal information as contemplated in this Code.[9]

1.6. The Code delineates the considerations that a responsible party is required to take into account in relation to the processing of personal information for purposes of access control and security management. It further prescribes the manner in which such personal information must be collected, used, stored and deleted ensuring that such processing is conducted in a lawful, reasonable, transparent manner and in accordance with the rights of data subjects as enshrined in POPIA.

2. BACKGROUND.

2.1. The initiative to develop the Code emanates from the need identified by the Regulator to address concerns and complaints raised by members of the public.

2.2. Members of the public have *inter alia* raised concerns that the collection of personal information at gated access entry points is excessive, not relevant and not limited to what is necessary in relation to the purpose for which it is processed

---

9 The Guideline to Develop Codes of Conduct in terms of Section 65 of the Protection of Personal Information Act, 2013 (No.4 of 2013)(hereafter referred to as Guidelines on Codes of Conduct)

as contemplated in POPIA and that such processing does not afford data subjects a reasonable opportunity to object to the processing of their personal information or to request further particulars regarding such processing in accordance with the provisions of POPIA.

2.3. The Regulator undertook research into the utilisation of closed-circuit cameras (CCTV) surveillance and in addition considered complaints received in this regard, which collectively revealed certain access control practices of an intrusive nature, including the processing of biometric information such as the use of facial recognition systems for the purpose of positive identification of data subjects. [10]

2.4. Furthermore, the deployment of CCTV surveillance at access control points results in the capture of facial images without the consent of data subjects and at times, without their knowledge or awareness. Such processing may constitute excessive collection and processing of personal information, in so far as it is not relevant and limited to what is necessary for the legitimate purpose for which it is collected and accordingly warrants the imposition of appropriate regulatory measures to ensure compliance with provisions of POPIA.

2.5. The Regulator is concerned with the collection of personal information of data subjects, whether effected manually, electronically or through a combination thereof, in circumstance where it is not clearly communicated where such information will be stored, the period for which it will be retained and *inter alia* whether it may be further processed. In light of these concerns, it imperative that the Regulator provide authoritative guidance on the lawful processing of personal information in accordance with POPIA, including the delineation of the consequences of non-compliance.

2.6. The Regulator acknowledges prior initiatives to develop a Code of Conduct addressing the processing of personal information at certain gated access points. Such proposals were limited in scope and sought to regulate only specific access control environments. These submissions were not approved, having failed to satisfy the requirements prescribed in the Guidelines for the development of Codes of Conduct. The Regulators own initiative Code of Conduct by contrast,

---

10 *'The use of CCTV cameras in South Africa and its compliance with POPIA'* - Research study concluded by the Information Regulator in 2023/24 financial year on (hereafter referred to as Regulators Research on CCTV). Also see the Data Privacy Code of Practice – Video Surveillance , Security Industry Association, 2022.

shall comprehensively govern or regulate the processing of personal information at all gated access points across diverse settings that constitutes restricted entry to a defined area, requiring authorisation or credentials for access, thereby ensuring compliance with the principles and obligations as set out in POPIA.[11]

2.7. Gated access encompasses the use of access control measures, including physical security personnel and other electronic systems, through which the personal information of data subjects is collected whether for security purposes or other legitimate reasons to regulate or restrict entry to premises under the control of a public or private body (responsible party). Such gated access measures include the deployment of CCTV surveillance at gated access entry points.

2.8. POPIA protects the personal information of all the data subjects including but not limited to, visitors[12], employees and residents who enter through gated access entry points.[13]

2.9. In accordance with the provisions of POPIA, the processing of Special Personal Information including biometric data such as fingerprints or facial images requires the implementation of heightened safeguards. Due to the inherently sensitive nature of such information and the potential for significant adverse impact on data subjects in the event of unlawful access, disclosure or processing, responsible parties must implement appropriate technical and organisational measures to secure such information and to prevent any unlawful or unauthorised processing in compliance with POPIA.[14]

2.10. The Code is intended to govern the processing of personal information in a manner that reconciles the legitimate objective of managing security risks at gated access points with the statutory and Constitutional rights of data subjects to privacy and the protection of their personal information as provided for under POPIA. It establishes principles to ensure that such processing is lawful, reasonable and proportionate to the purpose for which the information is collected.

---

11 https://www.google.com/search?q=gated+access+meaning&sca

12 Visitors include building contractors, service providers, drivers of delivery vehicles, casual labourers, family, and friends.

13 Standard Operating Procedures (SOP) for access control at the Bekronendreef entrance and exit gate to the Estate, Avonddans Country Estate.

14 Article 29 Data Protection Working Party; Opinion 3/2012 on developments in biometric technologies, 00720/12/EN WP193 (Working Party Opinion 3/2012) at 31

3. PURPOSE OF THE CODE OF CONDUCT.

3.1. This Code articulates the principles and prescribes the measures responsible parties are required to implement to ensure compliance with the eight (8) conditions for lawful processing of personal information, as well as any other provision of POPIA applicable to the processing of personal information collected at the gated access entry points.

3.2. The Code further set out specific obligations and provides guidance on the manner in which the conditions are to be applied or satisfied, having regard to the particular characteristics of the sector or the context in which the relevant responsible parties operate.[15]

4. OBJECTIVES OF THE CODE OF CONDUCT.[16]

The objectives of this Code are to:

4.1. provide clarity on the manner in which the conditions for lawful processing of personal information are to be applied and complied with, having regard to the particular characteristics of the relevant body, environment or sector;

4.2. provide appropriate mechanisms to give effect to the obligations associated with the conditions for the lawful processing of personal information;

4.3. stipulate appropriate standards and conditions for the lawful processing of personal information of specified personal information or classes of personal information or in respect of specified activities or classes of activities;

4.4. set out rules and procedures applicable to information matching programmes, where such programmes are utilised within the environment or sector as contemplated in this Code;

4.5. specify appropriate measures designed to protect the legitimate interests of data subjects;

4.6. provide for the duration and expiry of a Code; and

4.7. establish procedures for the submission, handling and resolution of complaints.

---

15 Section 60(2)(a)and (b) of POPIA

16 Guidelines on Codes of Conduct at para 6 at 8

5. SCOPE OF THE PROPOSED CODE

This Code applies to all the responsible parties that process personal information in the context of access control at gated access entry points, across both public and private sector environments. The scope of this Code extends to, but is not limited to the following settings:

5.1. Residential Buildings and Estates

These include "gated or walled communities being residential developments or housing estates characterised by controlled or restricted access to residents and authorised persons."[17]

5.2. Social Housing and Reconstruction and Development Programme (RDP) developments

These include social housing schemes and residential developments established under RDP initiatives, where access control measures are implemented to regulate entry to premises occupied by residents, beneficiaries and visitors, and where personal information is processed for such purposes.

5.3. Commercial Buildings and Complexes.

These include buildings, retail centres, multi-tenant complexes and hotels where access control measures are implemented to regulate the entry of employees, tenants, contractors, visitors and guests and where personal information is processed for entry to such premises.

5.4. Government and Other Buildings

These include premises occupied by organs of state that require heightened security measures to safeguard classified information and sensitive materials, and which typically employ layered access control systems in accordance with applicable security protocols, including where applicable, premises designated in terms of the National Key Points Act 102 1980.

5.5. Healthcare Establishments

---

17 https://stonewoodproperties.co.za/why-bodies-corporate-need-fidelity-insurance-for-sectional-title-buildings 07.04.25

These include hospitals, clinics, laboratories and similar facilities, where access control measures are necessary to ensure patient safety and protect the privacy of personal information while enabling secure and efficient access.

5.6. **Educational Institutions**

These include schools, colleges and institutions of higher learning where access control systems are implemented to regulate entry to campuses and facilities, balancing the need for accessibility with the obligation to ensure the protection of personal information of students, staff and visitors.

6. BINDING NATURE OF THE CODE.

This Code shall be binding on all the responsible party that processes the personal information of data subjects for purposes of access management or control, excluding those processing activities that fall within the scope of section 6 of POPIA or those that have been exempted in terms of POPIA.

7. LIMITATIONS/EXCLUSIONS

This Code is confined to the provisions that set out specific obligations of relevant bodies (responsible parties) bound thereby, as well as mandatory requirements prescribed under POPIA.[18]

8. COMPLIANCE WITH THE EIGHT (8) CONDITIONS FOR LAWFUL PROCESSING.

The proposed Code incorporates all conditions for the lawful processing of personal information and, where relevant, sets out obligations that provide a functional equivalent of all the obligations set out in those conditions.[19]

The responsible party who processes personal information at the gated access communities/premises has a duty to ensure compliance with the conditions for the lawful processing of personal information in respect of this proposed Code as outlined hereunder:

---

18 Guidelines on Codes of Conduct at 12.3.

19 Guidelines on Codes of Conduct at 13.1.2.

8.1. **Condition 1: Accountability**, **as referred to in section 8.**

8.1.1. In terms of section 8 of POPIA, the responsible party must in order to comply with the **conditions for lawful processing,** meet two requirements:

a) Firstly, appoint and register an Information Officer (IO) and where necessary a Deputy Information Officer (DIO)[20]. There is no limit to the number of DIOs that may be appointed.

b) The responsible party processing information at more than one gated access must ensure that the processing at each gated access is monitored, and the IO and or DIO's details are openly made known. The IO's role could be delegated to a person already holding a different role depending on the context per the Guidance Note on IO/DIO.

Example

In residential (gated communities) the following structures must decide who the information officer should be:

i. Body (bodies) Corporate.
ii. Trustees of body corporates
iii. Homeowners' Association (HOA).
iv. Heads of a public or private body.

c) Secondly, assign responsibilities for privacy and compliance with the Code of Conduct to a specific person who must be made known in terms of the provisions on openness. Responsibilities of the IO and DIO must align with the minimum standards set in the *Regulations Related to the Protection of Personal Information Act* (POPIA Regulations)[21] and will include the following actions:

i. To develop, implement, and continuously improve the compliance framework.

---

20 Guidance Note on Information Officer and Deputy Information Officer, Information Regulator, 2021, gives guidance on the registration process.

21 Regulations Related to the Protection of personal Information Act (POPIA Regulations). Regulation 4(1)(a)

ii. To monitor the implementation to ensure that there is compliance with this Code and with POPIA.
iii. To ensure that the compliance framework is maintained by reviewing it for applicability and relevance.
iv. To ensure that the Personal Information Impact Assessment (PIIA) is conducted before high-risk processing takes place.
v. Ensure that POPIA training is provided to all employees who are processing personal information of data subjects.

d) The compliance framework said above will include the following:
   i. Policies developed to ensure compliance with POPIA such as the-
      ii. Privacy Policy/statement/notice,
      iii. Retention Policy and schedule,
      iv. Incident Response Plan Policy,
      v. Information privacy and security policy,
      vi. other policies deemed necessary to ensure compliance with POPIA.

e) The documents in c) must specify the roles and responsibilities in the management of gated access (for example: role of security guards at the entrances responsible for collecting the information).

8.1.2. The IO and/or DIO must review the policies every three years or earlier should there be any need to do so.

8.1.3. To ensure compliance:

a) the IO/DIO must be able to demonstrate that there is compliance with the terms of the Code of conduct including ensuring that there are policies that: -

   i. Outline specific privacy expectations for employees (whether outsourced or contracted by operators or not).
   ii. Detail procedures for handling special personal information.
   iii. Establish reporting mechanisms for security compromises.
   iv. Establish how to implement security measures (e.g., encryption, access control).

v. Ensure implementation of regular privacy training for employees.[22]

8.2. **Condition 2: Processing limitation**, **as referred to in sections 9 to 12 of POPIA.**

8.2.1. **Section 9 (a) and (b).**

Personal information must be processed lawfully; and in a reasonable manner that does not infringe the privacy of the data subject.

a) The processing of information is lawful if the basis for its processing is based on any of the justifications provided for in section 11 of POPIA.
b) The personal information will be processed in a reasonable manner, where the "actions or decisions taken are fair, sensible, and appropriate given the circumstances" of the processing. [23]
c) An objective test will be applied to determine reasonableness and must be understood in the context of the Bill of Rights as a whole.[24]

8.2.2. **Section 10 on Minimality and Proportionality Test**

Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.

a) To determine that the personal information processed at the gated accesses is adequate and not excessive, the responsible party needs to assess the proportionality of each category of processed information in the light of the purpose for which the personal information is processed.[25]

---

22 https://www.infonetica.net/articles/privacy-and-Code-of-conduct-meaning#:~:text=Consent:

23 http://www.legalbriefai.com/legal-terms/reasonable.

24 Government of the Republic of South Africa and Others v Grootboom and Others (CCT11/00) [2000] ZACC 19; 2001 (1) SA 46 (CC); 2000 (11) BCLR 1169 (CC) (4 October 2000) Grootboom Case. At paragraph 44 page 34.

25 Article 29 Data Protection Working Party; Opinion 3/2012 on developments in biometric technologies, 00720/12/EN WP193 (Working Party Opinion 3/2012).

b) Proportionality Test: [26]

i. In analysing the proportionality of the processing against the purpose for collection of the personal information, the test must be conducted prior to its implementation,

ii. Necessary in relation to the purpose:-

In the case of a system to be implemented, such as a biometric system, the responsible party must assess "whether the system is necessary to meet the identified purpose. The system should be essential for satisfying that particular need rather than being the most convenient or cost effective.

iii. Likelihood of effectiveness:-

A second consideration is whether the system is likely to be effective in meeting the identified need by having regard to the specific characteristics of the system such the biometric technology planned to be used.

iv. Benefit outweighs loss of privacy:-

A third aspect to weigh is whether the resulting loss of privacy is proportional to any anticipated benefit. If the benefit is relatively minor, such as an increase in convenience or a slight cost saving, then the loss of privacy is not appropriate.

v. The processing that is excessive is deemed to be intrusive and in breach of the minimality requirement.

c) The following is the non-exhaustive list of categories of personal information for which a proportionality assessment must be conducted:

i. Unique identifiers (where more than one type is used)
ii. Special personal information (this includes all types)
iii. Personal information of children (especially where consent of a parent or competent person is not available)
iv. Vehicle related details.

d) In gated access contexts, proportionality assessments must be:

- **Premises specific**:

---

26 Working Party Opinion 3/2012 at page 7-8.

The minimal personal information processed should take account of scale, criticality, and throughput;

Example:

At a business park where employees enter at particular times in large numbers. The method of collection of the personal information should consider not just the convenience for entry at the gated access without balancing this against the necessity of the method, its effectiveness and the potential loss of privacy that may result due to the method (s) applied.

- **Purpose specific**,

  The processing of personal information must be aligned to clearly defined access objectives. Processing the exceeds the documented purpose would exceed the proportionality threshold and thus be excessive.

- **Documented**,

  The outcome of the proportionality assessment must be document and to form part of the risk assessment or impact assessment records; and

- **Reviewed periodically**,

  The outcome of the assessment must be reviewed regularly particularly where access patterns, technologies, or threats change.

Example of processing considered excessive/not proportionate:
The collection of multiple types of personal information of visitors, or contractors such as full names, contact number, vehicle registration number, identity number or driving license details, picture/image, biometric (fingerprint) for a single purpose of access control where alternative means are available such as where the access Code could be used to verify acceptance of the request to enter and to authorise such entry and exit.

Examples of <u>less excessive</u>/proportionate collection of information:[27]

i. The data subject entering the gated access being required to write their name to only be compared with the details on their ID book/card, passport or drivers' license;

ii. Visitors' vehicles entering gated accesses provided with a special permit or detachable sticker which should be checked on arrival before departing.[28] A unique number linked to the sticker/could in addition be provided to the driver to give it back on exit.

Examples of <u>less intrusive</u> verification of identity for the various categories of data subjects:

i. **Employees -** If not in possession of an access card, the employee may be made to complete the visitors' register and /or a visitor's access card may be issued, or the access cards or digital credentials linked to employee records that are already held by HR.

ii. **Visitors -** depending on the type of premises, a visitor could be provided access by receiving authorisation or have the visit confirmed to have taken place by the person being visited.

iii. **Pedestrians -** pedestrians could be verified using the method indicated above depending on what the reason for the entry through the gated access is[29]

e) Additional example per category of data subject is provided in *Table1.* below

8.2.3. **Scetion11 on Consent, justification and objection.**

In terms of POPIA Section 11(1) the personal information may only be processed if the processing is justifiable on the basis of one or more of the

---

27 Also see Appendix 1

28 Transnet Physical Access Control Standards

29 Transnet Physical Access Control Standards

6 grounds for lawful processing. Consent may not be the only justification for lawful processing, and this Code may not be construed to imply that:

a) Data subject consent as justification for the processing.

Consent must be informed, voluntary and an expression of will. POPIA does not provide for implied or indirect consent. The responsible party must ensure that measures are in place at gated accesses for compliance is in terms of the requirement of POPIA in the following manner (measures are not exhaustive) :

i. **Informed:**

The data subject must be made aware that consent is being obtained from them when that occurs or is intended.

The responsible party must be upfront about the personal information being processed and should provide clear information in a language that is understood by the data subject about how it will use personal information.

ii. **Voluntary:**

Consent is voluntary where amongst others, the method of obtaining consent from the data subject enables the data subject to exercise a choice of whether or not to give the consent.

Consent would not be voluntary if access is conditional on providing certain personal information (e.g., ID number, biometrics), as the data subject would not be allowed to exercise choice.

iii. **Expression of will:**

A written statement/register or online system whereby data subject accepts and consents to the processing of personal information by the responsible party must be substantially similar to Form 4 [30] prescribed in the POPIA Regulations.

30 https://inforegulator.org.za/wp-content/uploads/2020/07Form-4.pdf

iv. Consent must not be implied. There must be transparency when consent is being obtained.

Example of implied consent:
At the entrance of the gated access, there is a register that the visitor needs to complete and sign for purposes of gaining entry. When the data subject signs in the register, The responsible party assumes that the data subject has provided consent to process personal information without the data subject being informed.
The data subject may not be aware that by signing the register for purposes of gaining access to the buildings/yard/complex, they are deemed to be providing consent.

b) Contract as justification for processing personal information

i. The processing is justified if *it is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party.*[31]

ii. This justification may not apply in other gated access premises.

Example of when contract may be justification to process at a gated access.
Where the responsible party and the data subject enter into a contract, the data subject agrees to the processing of personal information for purposes outlined in the contract. This may include the management of entry to the complex/gate, providing boarding pass/ access card and employment contracts.[32]

iii. The responsible party in charge of the building, complex, office park or estate/Home-Owner's Association (HOA) bears the onus of proving that such a contract exists.

iv. The contract must be clear on how the information is going to be collected, stored, used, accessed, corrected and deleted.

---

31 Section 11(1)(b)
32 https://www.unittitles.govt.nz/assets/unit-titles/unit-titles-body-corp-operational-rules.pdf New Zealand

c) Obligation imposed by law on the responsible party as justification for the processing.[33]

i. The responsible party who is obliged to process personal information by law must make it known to the data subject at collection that such obligations as may affect the data subject exist;

ii. where the data subject has not consented to the processing, however the responsible party has an obligation in law to provide the personal information that it holds, which information is requested by the law enforcement agency. e.g., to investigate a crime.[34]

d) Legitimate interest of the data subject as justification for the processing:[35]

i. The processing of Personal Information is lawful if the responsible party in charge of gated access has objective proof that the processing protects the data subject.

ii. The legitimate interest to be protected can only be established after the responsible party has conducted a Legitimate Interest Assessment (LIA). The latter test is not outlined in POPIA. However, best practice in the regulation of privacy of personal information should be followed in applying this test to determine how the processing will protect the legitimate interest of the data subject. Some of the considerations during the LIA, which includes assessing:[36] -

i. The purpose test (identify helps to objectively identify a legitimate interest in the processing);

---

33 Section 11(1)(c) of POPIA.

34 Control Of Access To Public Premises And Vehicles Act, Act No. 53, 1985 8 May 1985

35 Section 11(1)(d) of POPIA.

36 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC

ii. The necessity test (to consider the connection between the processing and the interests pursued as well as purpose stated in the first test above); and

iii. The balancing test (consider the balance legitimate interest of that responsible party against the interests and rights of the data subject).

The LIA test should be used to assess the personal information of different data subjects like residents, employees, visitors, and contractors who need access to the gated accesses. The following link is attached to the Annexure **"A" -** Legitimate Interest Assessment Gated Access. This annexure provides a framework with minimum considerations to be made when conducting the LIA.

e) Proper performance of a public law duty by a public body as justification for the processing:

i. Only the responsible party who is a public body may be able to apply this provision to justify the processing of personal information.

ii. The public body must comply with the provisions of POPIA to ensure that the privacy of data subjects is always protected as may be relevant.

Example of a public law duty:

The government offices/departments need to monitor who enters the premises to maintain the safety and security of the state, which includes the following non-exhaustive list:-

i. South African Police Service Act, Act 68 of 1995
ii. (SAPS Act), provides for the establishment and regulation of SAPS. Section 14 of the SAPS Act empowers SAPS to 'preserve life, health, and property, which includes securing public premises and preventing crime'.
iii. Critical Infrastructure Protection Act 8 of 2019 which replaces the National Key Points Act 102 of 1980, establishes a framework for identifying and protecting critical infrastructure,

including access control and security obligations for public bodies.

f) Processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied as justification for the processing:[37]

i. The processing of personal information is lawful if the responsible party in charge of the gated access has conducted a LIA mentioned in (d) above to determine whether the processing pursues the legitimate interest of the responsible party or third party was made as a result of a LIA.

Example:

The legitimate interests could include, to detect and to prevent criminal activities or to monitor access for safety and other risk related reasons.

ii. The interest mentioned in d) and f) must be notified to the data subject at collection of the information.

iii. The responsible party must be transparent about the reason(s) why information at the gated access would be in the interest of the third party to whom the information is supplied.

NB. Publication of debtors' list is not in the legitimate interest of the responsible party nor the third party.

8.2.4. **Section 11(2) (a) and (b) of POPIA.**

a) Proof of consent.

The responsible party must keep proof of or the register of consent of data subjects in a secured manner.

b) Opportunity to withdraw

37 Private Security Industry Regulation Act, 2001 (Act 56 of 2001) Governs private security providers often contracted by public bodies for access control and guarding duties

The responsible party must afford data subject an opportunity to withdraw the consent provided.

8.2.5. **Section 11 (3) (a) of POPIA**

a) The data subject may object, at any time, to the processing of personal information where the justification for the processing of personal information is purported to protect the legitimate interest of the data subject in terms of Section 11(1)(d) and of the responsible party or third party in terms of Section 11(1)(f);

b) The objection should be based on reasonable grounds relating to the data subject's particular situation unless the legislation provides others.

c) The objection should be made in the prescribed manner. This could be in a manner that is substantially similar to Form 1 of the Regulations.[38]

d) The consequences of lodging an objection in terms of section 11(3) (a) such as refusal of access through the gated access must be clearly specified in the privacy notice that is made readily accessible to the data subject.

e) The responsible party must provide mechanisms to enable the data subject to object at the point of collection of personal information.

f) If the data subject has objected to the processing of personal information in terms of Subsection (3), the responsible party may no longer process the personal information. The responsible party must have systems in place to handle objections without denial of access to the premises such as offering alternatives that are not in breach of POPIA.

---

38 https://inforegulator.org.za/wp-content/uploads/2020/07/form-1-objection-to-the-processing-of-personal-information.pdf

Example

i. verification of identity.

8.2.6. **Collection directly from data subject as referred to in section 12.**

Personal information must be collected directly from the data subject. The data subject from whom the information may be obtained at entry at gated access includes visitors, contractors and suppliers.

The provisions of Section 12(2) of POPIA will not apply to the collection of personal information of the data subject for purposes of entry at gated accesses.

8.3. **Condition 3- Purpose specification**.

8.3.1. Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party.[39]

a) In cases of gated access, the primary purpose for collecting personal information should be specific to access control purposes to manage security risks.

Example:

to request persons to identify themselves at access-controlled entrances to buildings or areas.

b) The responsible party must ensure that it documents the purpose for collection of each type of personal information.

c) The responsible party must be able to make readily available to the data subjects and when required by the Regulator, the information about the purpose for each and every type of personal information that is collected including disclosure that the personal information is being and/or will be used by third parties.

Example:-

39 Section 13 of POPIA

If the responsible party requires the proof of identity using one or more of the following methods of processing of personal information, the purpose of each method as may be applicable, must be provided:-

i. Access card – linked to pre-recorded personal information.
ii. Identity Document (ID card/book) or passport.
iii. Drivers' licence.
iv. Licence disc details.
v. Fingerprint.
vi. Facial Recognition Technology (FRT).
i. Vehicle registration number

The responsible party must make the purpose clear where the information collected is to be used for linking personal information with the South African Police Service (SAPS) Licence Plate Recognition (LPR), the technology that is installed at gated access points (gated communities, residential estates, and business parks) as a critical tool for crime detection, prevention, and suspect apprehension. This system is often integrated with private security networks to enable real-time tracking of vehicles involved in criminal activities.[40]

NB: The processing of biometric information constitutes the processing of special personal information and will require compliance with section 26 of POPIA. Further considerations are outlined below.

8.3.2. **Retention and restriction of records as referred to in sections 14.**

a) The records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless—

i. retention of the record is required or authorised by law;

[40] LPR Cameras in Crime Prevention: A New Era in Crime Prevention, by MarketingDF, 4 March 2025.

ii. the responsible party reasonably requires the record for lawful purposes related to its functions or activities;
iii. retention of the record is required by a contract between the parties thereto; or
iv. the data subject or a competent person where the data subject is a child has consented to the retention of the record.

b) The responsible parties must have the Retention Policy and Retention Schedule in place**.** This policy and schedule detail the types of information processed, and the retention periods associated with each type of information. Whether there is a prescribed retention period by law or not, the responsible party must determine the appropriate retention period which is aligned to the operational needs of the responsible party and the type of personal information collected.

c) Retention period must be specific, including where the reason for the extended retention period is due to a specific request that was received from an appropriate law enforcement body (See Table 2 Gated Access Records: Purpose, Retention and Deletion Schedule).

d) During the retention period, personal information must be restricted for access and must only be retained and stored for purposes of the original purpose for which it was processed, and any further processing which is compatible with such purpose, such as for the purpose of provision of access and security.

e) The responsible party must be transparent about the format and location of the storage of information collected at gated accesses while in retention. This includes whether information is stored physically, electronically or digitally and where third parties' storage facilities used are located. It is best practice to have a cloud service provider agreement which will provide for compliance with POPIA including with Section 72(1).

f) Personal information collected for access control purposes is retained only for lawful operational or security requirements and is securely deleted once no longer needed, in line with the POPIA.

g) In terms of section 14 (4) of POPIA, the responsible party must destroy or delete a record of personal information or de-identify it as soon as reasonably practicable. Thereafter the responsible party is no longer authorised to retain the record in terms of subsection (1) or (2).

i. the responsible party must destroy or delete or de-identify when no longer needed. [41]

Personal information (such as access logs, visitor registers, or access Codes linked to individuals) must be deleted, destroyed, or de-identified as soon as it is no longer needed or lawfully allowed to be kept.

ii. The destruction or deletion of a record must be done securely[42]

When personal information is deleted or destroyed, it must be done securely, (prevents its reconstruction in an intelligible form) in any readable form so that it cannot be recovered or reconstructed.

iii. Restrict use in certain situations[43]

Access related personal information must be restricted (not actively used) if:

- A data subject challenges the correctness of the information (while it is being checked);
- The information is no longer needed, but must be kept only as proof (e.g. incident investigation);
- The information was unlawfully collected, and the data subject asks for restriction instead of deletion;
- The data subject requests their information to be transferred to another automated processing system.

iv. Limited Use While Restricted [44]

While information is restricted, it may only be:

- Stored (not actively used); and
- Used for proof, with consent, to protect someone's rights, or if required in the public interest.

---

[41] Section 14 (4)
[42] Section 14 (5)
[43] Section 14 (6)
[44] Section 14 (7)

v. Notify Before lifting the restriction[45]

If restricted personal information is going to be used again, the individual must be informed before the restriction is lifted.

8.4. **Condition 4- Further processing limitation as referred to in section 15.**

8.4.1. Further processing of personal information must be in accordance or compatible with the purpose for which it was collected in terms of section 13 of POPIA.[46]

Example:

The use of unique identifiers and linking them with that held by other responsible parties is possible where information is shared with the following categories of responsible parties (not exhaustive): -

a) Law enforcement bodies (agencies)
b) Operators

8.4.2. There may be an exchange of information between responsible parties and the operators such as security companies, close circuit television (CCTV) installation companies and law enforcement agencies.

8.4.3. In instances where further processing is compatible with the purpose for which the information was collected, the responsible parties are required to do the compatibility assessment test in terms of Section 15(2) of POPIA.

8.4.4. The further processing of personal information is not incompatible with the purpose of collection if: -

a) The data subject has consented to the further processing of the information.
b) In cases of children and minors, a competent person must have given the consent.

[45] Section 14(8)
[46] Section 15(1) of POPIA

8.4.5. Where it is necessary to further process personal information for purposes of law enforcement or as a result of an obligation imposed by law, or to a public body including for the prevention, detection, investigation, prosecution and punishment of offences; the circumstances under which this processing may take place need to be notified to data subjects at the time of collection.

8.4.6. The contractors, visitors or others who are not employees nor residents, should be notified of the possibility of further processing and must be given the opportunity to consent to the further processing of their personal information by the HOA. or Property management Agency as may be applicable except for further processing for law enforcement purposes.

8.5. **Condition 5- Information quality as referred to in Section 16.**

POPIA provides that the responsible party must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and where necessary updated.[47]

a) For the responsible party to ensure compliance, it must develop a system where the information collected is complete and accurate.

Example:

The responsible parties must require and/or provide mechanisms to the homeowners, residents, employees, tenants etc. (whose personal information has been processed) to verify and update the accuracy of their personal information every year.

8.6. **Condition 6: Openness as referred to in Sections 17 and 18.**

8.6.1. The responsible party must maintain the documentation of all processing operations under its responsibility as referred to in Section 14 or 51 of the Promotion of Access to Information Act 02 of 2000 (PAIA) in their website and offices.

[47] Section 16 (1) of POPIA

8.6.2. Notification to data subjects when collecting personal information in terms of Section 18 including but not limited to:

a) The responsible parties must notify data subjects on their Privacy Policy/statement/notice about the following:

i. For Section 18 compliance at gated accesses, the privacy notice must clearly cover:
ii. Who is collecting the information
iii. Why it is collected
iv. Whether provision is voluntary or mandatory
v. Who can access the information
vi. Rights of the data subject
vii. Right to complain to the Information Regulator

b) The Privacy Notice must also

i. Clear
ii. Visible
iii. Understandable
iv. Proportionate to the access context

8.7. Condition 7: Security safeguards as referred to in sections 19 to 22.

8.7.1. Security measures on integrity and confidentiality of personal information:
The responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent loss of, damage to or unauthorised destruction of personal information; and unlawful access to or processing of personal information.[48]
The responsible parties must have both organisational and technical measures to ensure the integrity and confidentiality of personal information.

This includes:

[48] Section 19. (1) of POPIA

a) identifying and managing the risks associated with the personal information of data subjects,
b) Developing directive policy on the way security safeguards determined by the risk mitigation measures, must be implemented and monitored by the responsible party implementing adequate security safeguards to mitigate the identified and known threats and risks to the personal information; and having the appropriate and adequately qualified information security personnel,
c) implementing adequate security safeguards to mitigate the identified and known threats and risks to the personal information; and having the appropriate and adequately qualified information security personnel.
d) Ensuring that vulnerability assessments or penetration testing is done to verify the effectiveness of the security safeguards.
e) documenting and testing incident response measures to be able to deal with security compromises in a manner that is consistent with POPIA. The incident response process/plan must be based on the adopted best practices

8.7.2. **Best practices on security measures to apply in managing access include but are not limited to:-**[49]

a) The responsible parties through the Code to adopt recognised information security best practices that they deem fit for their environment. Access to personal information that has been processed must be restricted to limited to persons who are authorised to access the Personal Information in order to perform their specific functions.
The following list of measures to adopt is not exhaustive:
b) Access is auditable viz. the network ID scanning system retains a record of everyone who logs in.
c) The network ID scanning system automatically deletes scanned personal information after 30 days.
d) Having a group password.
e) Training staff in their privacy obligations.

[49] Guideline 64: Privacy obligations for establishing and operating identification scanning systems

f) Keeping the networked ID scanning equipment secure by locking offices and ensuring the equipment is constantly supervised.

8.7.3. **Securing physical records:**

Measures to consider to secure paper-based records containing data subject Personal Information are not limited to the following:

a) Restricted Areas
b) Authorised Personnel
c) Visitor Protocols
d) Locked Storage
e) Regular Audits
f) Document Retention Policies
g) Reputable Shredding Companies for storage, deletion and destruction.

8.7.4. **Information processed by Operator or person acting under authority**

An operator or anyone processing personal information on behalf of the responsible party or an operator, must process such information only with the knowledge or authorisation of the responsible party; and treat Personal Information which comes to their knowledge as confidential and must not disclose it, unless required by law or in the course of the proper performance of their duties. [50]

The responsible party must have an operators' agreement with the security company or other third party that will conduct the services of managing the entry in the gated community/ commercial, business/government building.

8.7.5. **Section 21**

Security measures regarding information processed by operator.

i. The operator's agreement that the responsible parties has entered into with its operators must require the operator which processes

[50] Section 20 of POPIA.

personal information for the responsible party establishes and maintains the security measures referred to in section 19.[51]

ii. The operator must notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.[52]

iii. The operator agreement mentioned in above should include technical and organisational measures (TOMS) to be adopted by the operator. These measures must consider specialised requirements for Cloud Service Providers that may be used by the Operators providing electronic devices that are used to collect and store the personal information.

iv. The responsible party should ensure that these measures are verified independently through vulnerability assessments, audits, and penetration testing regularly to ensure that any new risks arising are identified and mitigated.

8.7.6. **Section 22**

a) **Duty to Notify**

The responsible party must notify:-

The Regulator, and the affected data subjects, as soon as reasonably possible that the personal information has been accessed or acquired by any unauthorised person, the responsible party.[53]

b) **Timing of Notification**

Notification may be delayed only if a public body responsible for crime prevention or national security determines that immediate notification would impede a criminal investigation.[54]

c) **Form and Manner of Notification**

The notification to data subjects must be communicated in a manner that is reasonably likely to reach them, which may include written

[51] Section 21 of POPIA.
[52] Section 21 of POPIA.
[53] Section 22 (1) (a) and (b) of POPIA
[54] Section 22 (3)

communication, electronic communication, public announcements, or other appropriate means.

d) **Minimum Content of Notification**[55]

The notification must provide sufficient information to enable affected data subjects to take protective measures, including:

i. A description of the possible consequences of the security compromise;

ii. The measures taken or proposed to address the compromise; and

iii. Recommendations on steps the data subject can take to mitigate potential harm.

e) The Regulator may direct the responsible party to publicise, in any manner specified if the Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the compromise.

f) **The Regulator's Oversight**

The Regulator may direct the responsible party on how and when to notify data subjects and may require additional information regarding the security compromise.

The Regulator has published guidelines for the submission of a security compromise notification through the e-services portal of the Regulator in terms of section 22 of POPIA that must be adhered to by responsible parties available on this link - https://eservices.inforegulator.org.za/compromises/docs/guide.pdf .

8.8. Condition 8: Data Subject participation as referred to in Sections 23 to 25.

The data subject has the right to have his, her or its personal information processed in accordance with the conditions for the lawful processing of personal information as referred to in Chapter 3:

[55] Section 22 (4) and (5)

8.8.1. **Access to personal information**[56]

establish whether the responsible party holds personal information of that data subject and to request access to his, her or its personal information as provided for in terms of Section 23.

a) Who May Request Access

Any resident, visitor, contractor, or service provider may request access to their own personal information held for access-control or security purposes, after proving their identity.

b) A data subjects may request:

i. Confirmation (Free of Charge)

Whether the estate holds any Personal Information about them (e.g. access logs, visitor records).

ii. Access to Their Information

A copy of, or description of:

- Visitor registers
- Access logs
- Entry and exit records
- Records showing who else (or which categories of people) had access to that information (e.g. security provider, managing agent)

iii. This access must be provided:[57]

- Within a reasonable time
- At a prescribed fee (if applicable)
- In a reasonable format
- In a way that is generally understandable

iv. **Right to Request Correction**[58]

- When access is given, the person must be informed that they have the right to:

[56] Section 23(1)
[57] Section 23(1)(b)
[58] Section 23 (2)

- Request correction, updating, or deletion of incorrect or misleading information.

v. **Fees and Deposits**[59]

If a fee applies:

- The estate must provide a written estimate of the fee in advance; and
- May require a deposit before processing the request.

vi. When Access May Be Refused[60]

The estate may or must refuse access where PAIA grounds for refusal apply, for example:

- Disclosure would reveal other people's personal information;
- Disclosure would compromise security or safety;
- Records are part of an investigation or legal process.

If only part of the record must be refused, the rest must still be disclosed (with redactions).

8.8.2. **Correction of personal information**[61]

The data subject request, where necessary, the correction, destruction or deletion of his, her or its personal information as provided for in terms of Section 24**.**

i. be notified of the details of the providers who collect and store the Personal Information.

ii. to establish whether a responsible party holds personal information of that data subject and to request access to his, her or its personal information as provided for in terms of Section 23;

iii. to request, where necessary, the correction, destruction or deletion of his, her or its personal information as provided for in terms of Section 24;

[59] Section 23 (3)
[60] Section 23 (4)
[61] Section 24(1)

8.8.6. **Manner of access**[62]

The provisions of Sections 18 and 53 of the PAIA apply to requests made in terms of Section 23 of this Act. In compliance with this provision the responsible party need to comply with the following measures:

i. Have a PAIA manual.
ii. Have PAIA request forms available.
iii. Treat POPIA access requests as formal PAIA requests.
iv. Verify identity before giving access.
v. Protect third-party personal information
vi. Respond within statutory timeframes

8.9. **Information Matching Programmes**

This Code specifies appropriate measures for information matching programmes as these programmes may be used in the context of this Code.[63]

8.9.1. For purposes of POPIA, an information matching programme occurs where there is the comparison, whether manually or by means of any electronic or other device, of any document containing personal information relating to ten or more data subjects, for the purpose of producing or verifying information that may be used for the purpose of taking any action in respect of an identifiable data subject.

8.9.2. Where a responsible party undertakes an information matching programme, such responsible party shall ensure that the processing of personal information is carried out in accordance with the provisions and conditions for the lawful processing of personal information as set out in POPIA.

8.10. **Automated Decision making**

8.10.1. A data subject may not be subject to a decision that:

a) is based solely on automated processing (i.e. with no meaningful human involvement);

[62] Section 25 of POPIA.
[63] Section 60 (4) (a) (i) of POPIA.

b) is intended to provide a profile of the data subject (e.g. work performance, creditworthiness, reliability, location, health, preferences, or conduct); and

c) results in legal consequences or

d) affects the data subject to a substantial degree.

8.10.2. **A decision has legal consequences when it:**

- Alters, creates, or extinguishes rights or obligations.
- Changes a person's legal status in a binding manner or
- Impacts data subjects' legal rights, e.g. being deprived of the right to citizenship.

8.10.3. **Substantial Degree of Impact**

Even without legal effect, a decision may still be prohibited if it:

a) Significantly affects the individual's circumstances, behaviour, or choices;

b) Has a prolonged or permanent impact; or

c) Leads to exclusion or discrimination.

8.10.4. **Examples of automated decisions that may have consequences for the data subject:**

a) Automatic access control decisions systems that:

Grant/deny entry based on cards, biometrics, license plates, QR Codes, mobile credentials.

Examples:

- A biometric gate that refuses entry because the fingerprint does not match.
- A licence plate recognition system that opens the boom gate only if the system authorises the vehicle.

b) Automated surveillance and alerts

Some gated communities or estates have:

- AI-based CCTV that flags "suspicious behaviour";
- Automatic number plate recognition (ANPR);
- Visitor vetting systems that auto-block certain users.

These are also automated decisions, especially where the outcome:

- restricts access;
- triggers law enforcement alerts;
- triggers security responses.

8.10.5. **Automated decisions may be permitted if:**

a) Automated Contractual necessity:
The decision is taken in connection with the conclusion or execution of a contract; and

b) The data subject's request is met or

c) Appropriate safeguards protect the data subject's legitimate interests.

8.10.6. **Mandatory Safeguards (POPIA s71(3))**

a) Where automated decisions are allowed: data subjects must be given an opportunity to make representations; and

b) Responsible parties must provide sufficient information about the underlying logic of the automated processing to enable the data subject to challenge and seek understanding of the processing.

8.11. **Personal Information of Children of unaccompanied minor**:

POPIA restricts the processing of the personal information of children unless authorisation in Section 35(1) is applicable. Where the access-control process depends on consent, the responsible party must obtain prior consent from a competent person in terms of Section 35(1)(a).

8.12. **Exemptions**:

The Regulator will consider applications for exemptions to process in breach of POPIA on a case-by-case basis depending on whether in the circumstances of the application, the public interest in the processing outweighs, to a substantial degree, any interference with the privacy of the data subject that could result from such processing; or the processing involves a clear benefit to the data subject or a third party that outweighs, to a substantial degree, any interference with the privacy of the data subject or third party that could result from such processing.[64]

---

64 Section 37(1)(a)and(b) of POPIA

8.13. **Special Personal Information**:

The types of Special Personal Information processed at gated accesses that are affected by this Code include biometric information of a data subject. POPIA restricts the processing of special personal information.[65] In the context of gated access, this restriction should be read against the provisions of Section 27(f), and the provisions of Sections 33 as the case may be.

9. GOVERNANCE, RISK & MONITORING OF THE CODE OF CONDUCT.

The responsible party bound by the Code must ensure that the Code is administered through their respective structures. [66] In the context of this Code, responsible parties bound by the Code include the specified body or class of bodies[67] namely, body (bodies).

Accountability provisions outlined in Condition 1 above apply to governance of the Code including establishment of the structures, processes, roles and responsibilities that ensure the Code is implemented effectively and that compliance with the Code is maintained. [68]

9.1. Each responsible party must ensure that in the governance structures are established and functional. Examples of responsible parties are not limited to the following:

9.1.1. Responsible Party: [69]

a) Residential Estates: could be the HOA or Body Corporate.

b) Public-sector owned premises: The public body[70], including a municipality or state-owned entity that is responsible for managing the premises.

c) Privately owned premises: The private body, private owner, landlord, or legal entity that owns and controls the premises.

---

65 Section 26 of POPIA

66 Bodies bound by the Code are listed above

67 Section 60 (3)(b) of POPIA

68 Paragraph 21 of the Guidelines at page 16

69 "public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information"

70 Public Body, Department or Organ of State3 (as defined in section 239 of the Constitution)

d) Commercial premises: The Chief Executive (CEO), Managing Director, or any designated person lawfully appointed as the head of the organisation.

9.1.2. Information Officers [71] will depend on the type of responsible party. This could be the Chairperson of the HOA (or Managing Agent if formally appointed).

9.1.3. Deputy Information Officer[72] will depend on the type of responsible party. This could be the Estate Manager or Security Manager (if designated).

9.1.4. **The governance structures and bodies bound by the Code that are responsible for the administration of this Code could be:**

a) Body corporate (including Trustees, Executive Estate Managers, Managing Agents, or any persons appointed under the Sectional Titles Schemes Management Act and related governance structures).

b) Board of governance in the public and private bodies (including Including executive boards, oversight committees, management boards and statutory councils).

c) Home-Owners Associations (Directors, elected committee members, and office bearers performing access control and estate management functions)

d) Associations in terms of Regulatory authorities such as Private Security Industry Regulatory Authority (PSIRA) or similar regulatory bodies.

e) Property Management Trading Entity (on behalf of state-owned entities).

f) Property Practitioners Regulatory Authority (including its appointed practitioners, inspectors, compliance officials, and administrative structures).

9.2. Monitoring of the Code [73]

---

71 Information Officers are, by virtue of their positions, appointed automatically in terms of PAIA and POPIA. Any person authorised as an Information Officer should be at an executive level or equivalent position.

72 Information Officers of public and private bodies must designate and/or delegate any power or duty to Deputy Information Officers

73 Paragraph 24 of the Guidelines at page 16. Also see ICO Data sharing Code page 78.

9.2.1. Oversight and monitoring by the Regulator.

a) The Regulator will monitor compliance with the Code of conduct as may be necessary in compliance with its mandate.

b) The responsible party is accountable for ensuring compliance with the Code and must be able to show that it is compliant with it[74] as such must have processes in place that outline how complaints or enquiries from data subjects will be handled and must assess compliance with the Code.

9.3. Monitoring of high-risk processing of personal information-the Risk Based Approach.

9.3.1. The high-risk processing may result in a high impact of harm on data subjects should there be a security compromise. As such the responsible party should prioritise conducting the PIIA as part of the risk management framework. *Gated Access Risk Management Framework,* Annexure **"B"** below outlines the risk management framework (RMF) as a minimum guide for the responsible parties who may not have adequate resources to develop the RMF.

9.3.2. Regulation 4(1)(b) places a responsibility on the Information Officer to conduct a PIIA. The purpose of the PIIA is to ensure that all necessary protections and safeguards are established before processing begins, aligning with POPIA's conditions for lawful processing of personal information.

9.3.3. The responsible party should conduct a PIIA to ensure that adequate measures and standards exist in order to comply with the conditions for lawful processing of personal information. [75]

9.3.4. Best compliance practice needs to be followed to use the PIIA in "identifying, assessing, and mitigating privacy risks associated with such processing," [76]

---

74 Paragraph 24.3 of the Guidelines at page 16
75 Regulation 4(1)(b) of the POPIA Regulations.
76 Guide to undertaking privacy impact assessments. May 2020 oaic.gov.au

A PIIA must assess the level of risk and whether certain types of processing or categories of information is 'high risk.'[77]

9.3.5. Monitoring high risk processing requires identifying the risk areas including risk of processing personal information through CCTV[78] which may potentially result in non-compliance with POPIA. Annexure **"B"** below provides a list of non-exhaustive question to provide guidance to responsible parties to assess potential areas of high-risk processing.

9.3.6. In identifying risk areas, the responsible party shall take into account the specific operating environment. Such considerations shall include, but not limited to, applicable risk profiles, throughput volumes, safety obligations and security requirements unique to residential estates, commercial complexes, healthcare facilities, educational institutions, and critical infrastructure environments.

10. REVIEW OF THE OPERATION OF CODE OF CONDUCT ISSUED AT OWN INITIATIVE

10.1. The Regulator may on its own initiative review the operation of the issued Code within a five (5) year period or as and when deemed necessary.

10.2. The review may occur when the Regulator becomes aware of, amongst others, the following:

10.2.1. a change in industry practices, technology or expectations of affected persons that may impact the effective operation of a Code; or

10.2.2. the lack of compliance with the issued Code.

10.3. The Regulator will notify the relevant body in writing of the decision to review the Code.

10.4. The Regulator will undertake a consultation during the review process.

---

77 https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance

78 Working Party set up under Article 29 of Directive 95/46/EC: Opinion 3/2012 on developments in biometric technologies Adopted on 27th April 2012.

10.5. If the Regulator decides to review Code of conduct issued at own initiative, the Regulator must publish a notice of the review on its website requesting comments from affected persons.

10.6. The outcome of the review of a Code may inform a decision by the Regulator to revoke an approved Code.

11. AMENDMENT AND REVOCATION

The Regulator may approve, in writing, a variation of an approved Code. A variation may occur on the Regulator's own initiative. [79]

11.1. The Regulator may amend or revoke a Code of conduct issued under Section 60 of POPIA [80]. In deciding whether to revoke an approved Code, the Regulator will consider the following:

11.1.1. a change in industry practices, technology or expectations of affected persons that may impact the effective operation of a Code; or

11.1.2. the lack of compliance with an approved Code.

12. NATIONAL AND/OR INTERNATIONAL APPLICATION

POPIA applies to the processing of personal information where the responsible party is domiciled in the Republic; or not domiciled in the Republic but makes use of automated and non-automated means in the Republic unless those means are used only to forward personal information through the Republic.

13. DATE OF COMMENCEMENT AND DATE OF EXPIRY

This Code of conduct as will be issued under Section 60 of POPIA comes into force on the 28th day after the date of its notification in the Gazette or on such later date as may be specified in the Code and is binding on every class or classes of body, industry, profession or vocation referred to therein.[81] The Code will remain effective for a period not exceeding five (5) years.

---

79 Paragraph 31.1.2 and 31.1.1 of the Guidelines

80 Section 64. (1) of POPIA

81 Section 62(2) of POPIA

14. REPORTING MECHANISMS.

14.1. The Regulator as the custodian of the Code of conduct should be made aware of the level of compliance of the responsible parties through the following means: -

14.1.1. Any person may submit a complaint to the Regulator in the prescribed manner and form alleging interference with the protection of the personal information of a data subject.[82]

14.1.2. The responsible party must submit the annual report about the effectiveness of the Code in compliance with the *Guidelines for Development of the Code*.[83]

15. COMPLAINTS MANAGEMENT[84]

15.1. The principles upon which the complaints about the processing of Personal Information at gated accesses may be made and handled include without limitations the following:-

15.1.1. The complaints process must be fair, transparent, and accessible to all data subjects. It must be easy to understand, publicly available, and provide for the prompt resolution of complaints. The process must clearly explain who may lodge a complaint, how a complaint can be submitted, and what reasonable assistance will be provided to enable a person to do so.

15.1.2. The complaint-handling processes must be at no cost on complainants, and that all complaint records are securely, accurately and efficiently captured and maintained.

15.1.3. The responsible party must ensure that it establishes the procedures and processes in compliance with the *Standard for Making and Dealing with Complaints in a Code of Conduct*, *prescribed in terms of section 65 of POPIA* to help enforce compliance with the approved Code of conduct as well as

---

82 Section 74 (1) of POPIA.
83 Paragraph 25 of the Guidelines
84 Standard For Making and Dealing with Complaints in a Code of Conduct (Prescribed in terms of section 65 of the Protection of Personal Information Act No 4 of 2013

other relevant legislative prescripts including but not limited to POPIA, PAIA and Promotion of Administrative Justice Act 3 of 2000 (PAJA).

15.2. Complaints to be lodged with the responsible party

15.2.1 Notice of procedure for making a complaint

The responsible party must clearly display information on how to lodge a complaint. This information must be:

- Visible at estate entrances or security offices;
- Available on the website (if applicable); and/or
- Included in printed notices or resident information packs.

15.2.2 The complaints procedure must clearly explain:

a) How to lodge a complaint
for example, by email, online, or in writing at the security office.

b) Who receives the complaint
the name or role and contact details of the person responsible for receiving and acknowledging complaints must be included.

c) How the complaint will be handled, including:
   i. How the complainant will be kept informed of progress;
   ii. The expected timeframe for resolving the complaint;
   iii. How and when the complainant will be informed of the outcome and reasons for the decision;
   iv. Under what circumstances will the complaint be referred to the adjudicator and or to the information regulator.

d) Remedy or corrective action may be provided by the responsible party. Depending on the complaint raised, the following are without limitation examples of remedies that may be provided by the responsible party.

   i. Correction, deletion, or destruction of personal information.
   ii. Granting access or responding to POPIA rights.
   iii. Stopping unlawful or excessive processing.
   iv. Improving security measures.
   v. Updating privacy notices and procedures.
   vi. Providing written acknowledgement and outcomes.
   vii. Ensuring accessible objection/complaints channels.
   viii. Retraining or disciplining personnel.

15.2.3 **Escalation options, including:**

a) When a complaint may be escalated to the Regulator;

b) The complainant's right to refer the matter to an independent adjudicator if dissatisfied with the outcome;

c) How and within what timeframe a complaint may be referred to an independent adjudicator;

d) Contact details of the independent adjudicator.

15.3. Appointment of the adjudicator

15.3.1 To comply with POPIA and provide an effective complaints handling mechanism, each responsible party operating a gated access point must appoint or designate an adjudicator. The adjudicator must be independent, impartial and competent to resolve complaints arising from the processing of personal information arising at gated access points.

15.3.2 In the residential sector, including estates, complexes and Reconstruction and Development Program (RDP) settlements with gated access points, the adjudicator may be appointed by the governing management body or a recognised property regulatory authorities/bodies such as the Community Schemes Ombud Services (CSOS), National Association for Managing Agents (NAMA) or the Residential Communities Industry (RCI) provided that the adjudicator is independent and capable of performing the functions set out in this Code.

15.3.3 In the commercial sector including office parks, government buildings and industrial or mixed-use premises, the responsible party shall appoint the adjudicator directly, through an independent third party or recognised property management entities such as the Property Management Trading Entity on behalf of state-owned entities to perform the functions set out in this Code.

15.3.4 The adjudicator must act independently and impartially and must be appropriately skilled to adjudicate complaints in accordance with POPIA.

15.3.5 Any data subject or responsible party aggrieved by a determination of the adjudicator may in terms of section 74(2) of POPIA, refer the matter to the Regulator for determination.

15.3.6 Each responsible party shall publicly communicate the details of the adjudicator and the procedure for lodging complaints, ensuring transparency and accessibility for data subjects.

15.4. Handling of Complaints by the Information Regulator

Lodging a complaint with the Regulator.

15.4.1 The data subject should make use of the Form 5 prescribed by the Regulator to lodge a complaint about the responsible party who does not comply with this Code of conduct.

15.4.2 When filling in Form 5 (the complaint form), the data subject should include in the following:

a) full details of the complainant (full names, address and contact details)

b) full details of the responsible party (full names, address and contact details)

c) brief description of the matter and why you think the responsible party has processed your Personal Information in contravention of POPIA.

d) any further documentation or information that may support your complaint (screenshots, documents, recordings etc.).

e) ensure that the complaint form is signed and dated.

f) further details on how to lodge a complaint can be found in the Rules of Procedure for handling of complaints by the Regulator available on this link https://inforegulator.org.za/wp-content/uploads/2020/07/20211012-InfoReg-RulesOfProcedure-HandlingPOPIAcomplaints.pdf and POPIA.

g) the details of a channel through which a complaint must be lodged *viz*: POPIA Division of the Information Regulator is responsible for handling the complaints and will be reached at popiacomplaints@inforegulator.org.za

15.4.4. To access this service, the user must first register a user profile on our eService Portal and submit the complaint through the Portal.

Should a data subject or responsible party require further clarity on complaints, the Regulator may be reached on POPIAComplaints@inforegulator.org.za

15.5. Investigation Proceedings of Regulator

15.5.1. The Regulator will receive and investigate complaints received from the responsible party or the data subject in terms of section 63(3) of POPIA, if aggrieved by the determination of an adjudicator.

15.5.2. In terms of section 81 of POPIA, for the purposes of the investigation of a complaint the Regulator may—

a. summon and enforce the appearance of persons before the Regulator and compel them to give oral or written evidence on oath and to produce any records and things that the Regulator considers necessary to investigate the complaint, in the same manner and to the same extent as the High Court;
b. administer oaths;
c. receive and accept any evidence and other information, whether on oath, by affidavit or otherwise, that the Regulator sees fit, whether or not it is or would be admissible in a court of law; at any reasonable time, subject to section 81, enter and search any premises occupied by the responsible party;
d. conduct a private interview with any person in any premises entered under Section 84 subject to section 82; and
e. otherwise carry out in those premises, any inquiries that the Regulator sees fit in terms of section 82.

15.6. **Review a decision after a complaint has been finalised:**

Should a person be dissatisfied with the decision and reasons provided, an application should be made within 14 (fourteen) days from the date of the decision to the Regulator by completing Form 20, which can be found in this link to the website of the Regulator.
https://inforegulator.org.za/wp-content/uploads/2020/07/20211012-InfoReg-RulesOfProcedure-HandlingPOPIAcomplaints-1.pdf

Table 1: Examples of minimal vs excessive personal information.

Category	Minimal / Necessary (Compliant)	Excessive / Unnecessary (Non-Compliant)
Employees	- Name - Employee ID / Access Card Number - Time of entry/exit	- Full ID number - Home address - Personal phone number - Next of kin details - Biometric data (if not justified)
Visitors	- Name - Purpose of visit - Vehicle registration (only if driving in) - Time of entry/exit	- ID copy or photo - Home address - Email address - Personal phone number - Employer details
Contractors	- Name - Company name - Work order reference - Time of entry/exit	- Full ID number - Bank details - Residential address - Emergency contact info
Retention Period	- Logs kept for security audit period (e.g., 30 days)	- Indefinite retention of logs - Storing data beyond legal or operational need

Table 2 Gated Access Records: Purpose, Retention and Deletion Schedule

This schedule is aligned to section 14 of POPIA and reflects a purpose-based approach to retention and deletion of personal information processed through gated access controls.

Record type	Purpose	Ideal retention period	Deletion / disposal rule
Visitor registers (manual/electronic)	Verify entry/exit; trace visitors for security incidents; resolve access disputes	30–90 days (up to 6 months if risk-justified)	Securely delete/shred after retention period unless the record is flagged for an incident or investigation, in which case it is retained with the incident file
Resident/employee access profiles	Maintain ongoing access rights; identity verification; administration of access privileges	Duration of residency/employment + 30–90 days	Disable access immediately on exit; delete or de-identify after grace period unless required for an active dispute, audit, or legal matter
Access card/tag issuance and return records	Asset control; accountability for access devices; audit trail	12 months after return or deactivation	Delete after retention period; retain only minimal de-identified audit metadata if necessary
Access control system logs (swipe/scan logs)	Monitor access points; detect unauthorised access; reconstruct movements during incidents	30–90 days (up to 6–12 months for high-risk sites)	Automatically purge on a rolling basis; if linked to an incident, retain relevant extracts with the incident record
CCTV footage	Deter crime; support investigations; provide evidence	7–30 days	Automatically overwrite after cycle; export and retain only footage linked to an

	for disciplinary or criminal matters		incident, then delete after the incident retention period
Incident / occurrence reports	Risk management; corrective action; legal defence; reporting to insurers or authorities	3–5 years	Delete or de-identify after period provided there is no active litigation, claim, or legal hold
Contractor/service provider access records	Track third-party entry; accountability; incident investigation	6–12 months after contract completion	Delete after retention period unless linked to an incident, in which case retain with the incident file
Access authorisation approvals	Governance; proof of delegation; audit trail for access decisions	3–5 years	Delete after retention period unless retention is required for audit or legal purposes

Annexure "B": Gated Access Risk Management Framework.

Gated Access Risk Management Framework

1. Purpose and Scope

This framework provides a structured approach to identifying, assessing, and managing risks associated with gated or controlled access environments, including estates, office parks, campuses, and secure facilities. It addresses physical security, operational processes, information protection, and legal compliance.

2. Governance and Oversight

Effective gated access risk management requires clear accountability, senior management oversight, defined operational roles, and documented policies. Governance should ensure alignment with organisational objectives and legal obligations.

3. Risk Assessment Methodology

The framework applies ISO 31000 risk management principles: establishing context, identifying risks, analysing likelihood and impact, evaluating existing controls, and implementing risk treatment plans.

The **Risk and Control Matrix (RACM) is a standard approach that** allows organisations to visualise and evaluate the effectiveness of their risk control strategies and make data-driven decisions to enhance their risk management practices. The RACM typically includes the following components:[85]

Risk identification: The matrix lists all the potential risks an organization may face, often categorized by business areas, processes, or functions.

Risk assessment: Each identified risk is assessed based on its likelihood of occurrence and potential impact on the organization. This assessment helps prioritize risks and focus resources on the most critical areas.

Control measures: The matrix outlines the specific control measures implemented to mitigate or reduce the likelihood and impact of each risk. These measures can include policies, procedures, systems, or other mechanisms.

[85] https://www.investopedia.com/terms/r/risk-control.asp (Investopedia)

Control effectiveness: The RACM evaluates the effectiveness of each control measure, taking into account factors such as the level of compliance, the adequacy of the control design, and the control's ability to detect or prevent the risk from materializing.

Action plans: The matrix is based on the assessment of control effectiveness and may include action plans for improving risk control measures or addressing identified gaps in the organization's risk management practices.

4. Key Risk Categories

Key risks managed by access control include physical intrusion(unauthorised entry), tailgating, system failures, insider threats, data protection breaches, non-compliance with POPIA, and failures by contracted security service providers:

1. Security Risks (Unauthorised Access)

Intrusion and Trespassing: Preventing unauthorized individuals from entering buildings or restricted areas.

Theft and Vandalism: Protecting valuable equipment, assets, and inventory from theft or damage.

Information Theft/Espionage: Preventing unauthorized access to confidential, sensitive, or classified information (data leaks).

Social Engineering: Mitigating risks from individuals attempting to gain access through deception. [86][87]

2. Operational and Safety Risks

Unaccounted Visitors/Contractors: Managing risk related to unauthorized or unvetted individuals on-site, which can lead to liability issues.

Employee Safety: Protecting staff from physical harm by controlling who has access to the workplace.

Health and Safety Hazards: Restricting access to dangerous, specialized, or restricted areas (e.g., server rooms, laboratories, high-voltage areas).

3. Compliance and Liability Risks

Breach of Duty of Care: Ensuring compliance with occupational health and safety regulations (e.g., Occupiers' Liability Act) by restricting access to authorized individuals.

[86] https://www.investopedia.com/terms/r/risk-control.asp
[87] auditboard.com

Regulatory Non-compliance: Meeting legal requirements for data protection (e.g., GDPR) and industry-specific security standards. [88]

5. Risk Control Measures

Risk control is a set of methods by which firms evaluate potential losses and take action to reduce or eliminate such threats. The technique uses findings from risk assessments that involve identifying potential risk factors in a company's operations. These can include technical and nontechnical aspects of the business, financial policies, and other issues that may affect the well-being of the firm

Controls should be layered and include physical barriers, access control technologies, standard operating procedures, staff training, monitoring, incident response, and privacy safeguards.

A risk matrix should be used to determine the exact levels of layers of security required.

Multiple layers of security must be justified in terms of risk assessment evidence.

Typical Access Control Mechanisms

Physical Barriers: Fences, gates, and turnstiles.

Electronic Security: Access cards, biometric scanners, and PIN pads.

Personnel Measures: Security guards, receptionists, and visitor management systems.

Procedural Controls: Key management and escorting visitors

6. Information Protection and POPIA Compliance

Personal information processed at access points must be lawful, minimal, secure, and transparent. Retention periods must be defined, operator agreements in place, and data subject rights supported.

FAIR (Factor Analysis of Information Risk)**:** Focuses on evaluating frequency and magnitude of loss.

7. Incident Management and Business Continuity

Incidents must be documented, escalated, investigated, and used to improve controls.

Business continuity planning ensures gate operations can continue during power, system, or security disruptions.

8. Monitoring, Review, and Improvement

[88] Aon South Africa

Key risk indicators, audits, and periodic reviews support continual improvement and ensure risks remain within acceptable appetite.

Annexure "C" High Risk Processing Checklist (POPIA)

1. Type of Personal Information

☐ Are you processing special personal information (e.g. race, health, biometric, religious beliefs)?

☐ Are you processing children's personal information?

☐ Are you processing criminal behaviour or records?

2. Scale and Scope

☐ Is the processing done on a large scale (e.g. thousands of data subjects)?

☐ Is the processing systematic or ongoing (e.g. continuous monitoring)?

3. Technology Used

☐ Are you using automated decision-making tools (e.g. AI, algorithms)?

☐ Are you using biometric systems (e.g. facial recognition, fingerprint scanning)?

☐ Are you using emerging technologies (e.g. IoT, smart devices)?

4. Impact on Data Subjects

☐ Could the processing result in discrimination, identity theft, or reputational harm?

☐ Could it affect the rights or freedoms of individuals?

☐ Is there a risk of financial loss or denial of services?

5. Data Transfers

☐ Are you transferring personal information outside South Africa?

☐ Is the destination country not subject to adequate data protection laws?

6. Monitoring and Surveillance

☐ Are you conducting systematic surveillance (e.g. CCTV, employee monitoring)?

☐ Are you tracking online behaviour (e.g. cookies, profiling)?

7. Consent and Transparency

☐ Is the processing not based on explicit consent?

☐ Are data subjects not fully informed about how their data is used.

8. **Operational environment**

Are there clear identifiable security risks, duty-of-care obligations, and liability burden in the environment such as the following-

☐residential estates,

☐commercial complexes,

☐ healthcare facilities,

☐educational institutions, or

☐critical infrastructure environments.

Sources of References

1. Access control standards for security officials operating at access and egress control points, Transnet Physical Access Control Standards.
2. Advertising and marketing industry Code of conduct No. 40159 Government Gazette, 26 July 2016
3. CCTV Code of Practice, Information Commissioner's Office, 2008.
4. Code Of Conduct Prescribed Under the Private Security Industry Regulation Act, 2001 (Act No. 56 Of 2001), Code of Conduct for Security Service Providers, 2003
5. Code of conduct, The Office of the Consumer Goods and Services Ombud ("the CGSO") is the Consumer Goods and Services Industry's voluntary Ombud scheme set up in line with the Consumer Protection Act 68 of 2008.
6. Code Of Conduct for All Legal Practitioners, Candidate Legal Practitioners and Juristic Entities.
7. Code of Conduct Confidentiality, Privacy and Data Use Policy February 2024. Carbon Market Institute, Australia ('CMI').
8. Code Of Conduct for Victorian Public Sector Employees Of Special Bodies, Victorian Public Sector Commission.
9. Code Of Conduct, The Office of the Consumer Goods and Services Ombud ("the CGSO") is the Consumer Goods and Services Industry's voluntary Ombud scheme set up in line with the Consumer Protection Act 68 of 2008.The Consumer Goods and Services Industry.
10. Data Privacy Code of Practice – Video Surveillance , Security Industry Association, 2022
11. European Data Protection Board: Guidelines 3/2019 on processing of personal data through video devices Version 2.0 Adopted on 29 January 2020.
12. European Data Protection Board: Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR(the pursuit of a legitimate interest) Version 1.0 Adopted on 8 October 2024.
13. European Data Protection Board: Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0 Adopted on 20 October 2020.
14. European Data Protection Board: Document on the procedure for the development of informal "Codes of Conduct sessions" Adopted on 10 November 2020.
15. Fact Sheet Captured on Camera Street level imaging technology, the Internet and you
16. Information and Privacy Commissioner for British Columbia www.oipc.bc.ca
17. Information Commissioner's Office Consultation: Age-Appropriate Design Code.

18. Guidance on video Surveillance including CCTV, UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). 17 October 2022 - 1.0.21.
19. New South Wales Government policy statement and guidelines for the establishment and implementation of closed-circuit television (CCTV) in public places: NSW Government Initiative, 2014.
20. Office of the Australian Information Commissioner (OAIC) (n.d.) *ID scanning*. Available at: https://www.oaic.gov.au/privacy/your-privacy-rights/surveillance-and-monitoring/id-scanning (Accessed: 8 September 2025).
21. Pecanwood Estate HOA Egress Control, Vetting and Enrolment Policy, April 2021.
22. Policy Brief the Use of CCTV Cameras In South Africa And Its Compliance with Popia November 2024.
23. Privacy and CCTV, A Guide to businesses, agencies and organisations, Office of the Privacy Commissioner, New Zealand.
24. Research study concluded by the Regulator in 2023/24 financial year on 'The use of CCTV cameras in South Africa and its compliance with POPIA' United Kingdom: Anthony Woolley and Deborah Woolley against Nahid Akbar or Akram A436/16 ([2017] SC EDIN 7).
25. Republic of South Africa. (2011) Sectional Titles Schemes Management Act, No. 8 of 2011. Pretoria: Government Printer. Available at: https://www.gov.za/documents/sectional-titles-schemes-management-act (Accessed: 8 September 2025).
26. Security Industry Association, Data Privacy Code of Practice – Video Surveillance, 2022.
27. Standard Operating Procedures (SOP) for access control at the Bekronendreef entrance and exit gate to the Estate, Avonddans Country Estate 2 April 2024.
28. South African Intruder Detection Services Association (SAIDSA) By-Law No. 9 Requirements for the Installation of a Video Surveillance System (VSS).
29. Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012 (PoFA) Home Office, for England and Wales.
30. 'The use of CCTV cameras in South Africa and its compliance with POPIA' - Research study concluded by the Information Regulator in 2023/24 financial year on (hereafter referred to as Regulators Research on CCTV).
31. Transnet (2022) Access control standards for security officials operating at access and egress control points: Transnet Physical Access Control Standards. [Online]. Available at: [https://www.etenders.gov.za/home/Download/pdf] (Accessed: [20 December 2024).
32. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data

and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

33. Working Party was set up under Article 29 of Directive 95/46/EC. Advice paper on special categories of data ("sensitive data")
34. Working Party set up under Article 29 of Directive 95/46/EC: Opinion 3/2012 on developments in biometric technologies Adopted on 27th April 2012.
35. Working Party set up under Article 29 of Directive 95/46/EC: Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC Adopted on 9 April 2014
36. Working Party set up under Article 29 of Directive 95/46/EC: Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Revised and Adopted on 6 February 2018.
37. Working Party set up under Article 29 of Directive 95/46/EC: Opinion 02/2012 on facial recognition in online and mobile services. Adopted on 22 March 2012
38. Working Party set up under Article 29 "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679". WP 248 rev.01, 4 October 2017. ec.europa.eu/newsroom.
39. Working Document on the Processing of Personal Data by means of Video Surveillance Adopted on 25 November 2002.

Risk Management Framework Reference Sources

1. ISO 31000:2018 – Risk Management — Guidelines (International Organization for Standardization).
2. ISO 22301:2019 – Security and Resilience — Business Continuity Management Systems (ISO).
3. Protection of Personal Information Act 4 of 2013 (South Africa).
4. Information Regulator: Guidance and sectoral developments on gated access processing.
5. Private Security Industry Regulation Act 56 of 2001 (PSiRA).
6. Michalsons: Gated Access Code of Conduct under POPIA.
7. ITLawCo: POPIA Code of Conduct for Gated Access Analysis. (https://itlawco.com/popia-Code-of-conduct-gated-access-south-africa/)

APPENDIX 1

Data Collection Minimality Practices at Gated Access

Category	Minimal / Necessary (Compliant)	Excessive / Unnecessary (Non-Compliant)
Employees	- Name - Employee ID / Access Card Number - Time of entry/exit	- Full ID number - Home address - Personal phone number - Next of kin details - Biometric data (if not justified)
Visitors	- Name - Purpose of visit - Vehicle registration (only if driving in) - Time of entry/exit	- ID copy or photo - Home address - Email address - Personal phone number - Employer details
Contractors	- Name - Company name - Work order reference - Time of entry/exit	- Full ID number - Bank details - Residential address - Emergency contact info
Retention Period	- Logs kept for security audit period (e.g., 30 days)	- Indefinite retention of logs - Storing data beyond legal or operational need