CELCOM (PTY) LTD

ISO 9001 2015

QUALITY MANAGEMENT SYSTEM

PROCEDURE	PROCESS NUMBER:	QMProcC 01-76b-01
POPI MANUAL **Regulations relating to the Protection of Personal Information and the Protection of personal information act**	DATE:	29 June 2021
	VERSION:	0001

PREPARED IN TERMS OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013(ACT 4OF 2013) WITH SPECIFIC REFERENCE to Section 2 to 38; Section 55 to 109 and Section110 and 114(4) OF THE ACT

PURPOSE:	To have a working policy in place that defines the Protection of personal information in terms of obtaining information, usage, storage and destroying of records

PROCEDURE	Responsibilities
"POPIA" THE PROTECTION OF PERSONAL INFORMATION ACT	• The POPI Act is a new all-inclusive piece of legislation, a privacy law, that safeguards the integrity and sensitivity of private information. Companies are required to carefully manage the data capture and storage process of Personal Information.

POPI Act Compliance

Failure to comply with the requirements of the POPI Act could have dire consequences.

Although one cannot and should not shy away from the legal aspects of the Act, POPIA should be seen as an opportunity to identify, clean-up and manage information better, and in doing so, improve business processes.

Do not fall into the trap of implementing POPIA just to meet your compliance requirements.

Steps to take Immediately

Download the Act and draft regulations and become familiar with them.

Protection of Personal Information Act 4 of 2013 | South African Government (www.gov.za)- (A copy is in office and will be distributed with training)

Review all the pages on this website and keep in touch as this will be updated frequently.

Appoint an Information Officer and ensure that he is aware of his roles and responsibilities.

Make decision makers and key personnel in your organization aware that the law has changed in accordance with the POPI Act and the severe consequences of non-compliance.

Conduct a current status risk assessment / information audit to establish data protection compliance level.

Document what Personal Information you currently hold, where it comes from, how it is to be used and who you share it with.

Produce a POPI Act policies and procedures manual and ensure that everyone who deals with Personal Information is aware of the legal implications of this Act. This manual is to include your organizations privacy policy with regard to:

- Data collection (type of data, purpose, consent, legal aspects, minimality, and transparency) Data access and accuracy (correct, complete, reliable and process of updating information)
- Data usage and restrictions (purpose, relevance, restrictions, legality, permission, limitations)
- Data storage (physical, off-site, electronic, back-up, cloud storage)
- Data security safeguards (physical, electronic, network, password control, disaster recovery. Disclosure (legality, consent, data subject awareness, data request handling)
- Responsibilities (All directors, top management, Information Officer, personnel dealing with Personal Information, vendors, contractors, suppliers)
- Complaints (process, handling, legalities, transparency)
- Retention (retention schedule) Destruction (destruction schedule) Implement staff awareness training (all current staff, new appointees and regular refresher training).

Procedures are put in place to monitor and enforce compliance.

Relationship with other Acts

The POPI Act (POPIA) is just one of many Acts that govern South African law. When looking at the requirements of the POPI Act, the requirements of other Acts should also be taken into consideration.

The Protection of Personal Information Act (POPIA) and the Promotion of Access to Information Act (PIAI) hold a special relationship. Both can be seen as "information" laws and are each on one end of a continuum. On the one end, PAIA is an "Access" law, all about Freedom of Information. POPIA on the other end, is about Privacy - prevention of exposure of information. Do not see them as competing, both are there to help ensure that information is managed correctly.

Below are some of the other Acts that may impact the POPI Act compliance process.

- Basic Conditions of Employment Act 75 of 1997
- Broad-Based Black Economic Empowerment Act 53 of 2003
- Close Corporations Act 69 of 1984
- Companies Act 71 of 2008
- Compensation for Occupational Injuries and Diseases Act 130 of 1993
- Consumer Protection Act, No 68 of 2008
- Copyright Act 98 of 1978
- Electronic Communication and Transactions Act 25 of 2002
- Income Tax Act 58 of 1962
- Intellectual Property Rights from Publicly Financed Research and Development Act 51 of 2008
- International Standard for Records Management (ISO15489)
- Labour Relations Act 66/1995
- National Archives and Records Service of South Africa Act 43 of 1996
- National Credit Act 34 of 2005
- Promotion of Access to Information Act 2 of 2000 (PAIA)
- Promotion of Administrative Justice Act 3 of 2000 (PAJA)
- Protection of Personal Information Act 4 of 2013 (POPI)
- South African National Standard for Records Management (SANS 15489)
- The Constitution of the Republic of South Africa 1996
- Value Added Tax Act 89 of 1991

In addition to these Acts, other Industry specific Act, Regulations, Codes of Practice should be considered. In particular, the King Report on Corporate Governance, (King III and IV) should be considered.

KEY DEFINITIONS

- “Data subject” – a person to whom personal information relates.
- “Direct marketing” – sending a data subject an electronic communication about goods and services that you are promoting or offering to supply in the ordinary course of business or requesting a donation of any kind for any reason.
- “processing” – any operation or activity concerning personal information.
- “record” – any recorded information, regardless of when it came into existence.
- “Responsible party” – a public or private body or any other person which determines the purpose of and means for processing personal information.

For a full list of definitions, please refer to the POPI Act which can be downloaded from Act No. 4 of 2013 : Protection of Personal Information Act, 2013

The POPIA Act Applies to Everyone

The Act applies to any person or organisation who keeps any type of records relating to the personal information of anyone, unless those records are subject to other legislation which protects such information more stringently.

It therefore sets the minimum standards for the protection of personal information. It regulates the "processing" of personal information. "Processing" includes collecting, receiving, recording, organizing, retrieving, or using such information; or disseminating, distributing or making such personal information available.

The Act will also relate to records which are already in the possession of the entity or person doing the processing, the storage and ultimately the manner in which information is destroyed and discarded.

This article must be read in conjunction with the POPI Act which can be downloaded from Act No. 4 of 2013 : Protection of Personal Information Act, 2013

What POPIA means for business

The POPI Act ensures that the right to privacy is taken seriously and includes a data subject's right to be protected against any unlawful collection, retention, dissemination and use of their personal information.

Companies are required to receive consent from individuals before they can obtain, retain and process personal information for communication or any other purpose. As per "Conditions for lawful processing" the definition of "Personal Information" includes contact details, demographic information, personal history, as well as communication records.

The POPI Act highlights the need for a greater understanding of the way in which personal information is stored and processed. This means that the systems, processes and how logical and physical access is maintained and managed for the systems and areas housing personal information al need to be considered.

Protection of Personal Information requires extra vigilance in all aspects of physical and information security. The basis of the POPI Act is to protect personal information and prevent information from being exposed to unauthorised persons. As a result, this implies an obligation to protect information relating to individuals and juristic entities from any damage, including financial fraud, identity theft, misuse and the abuse of personal information.

The POPI Act requires that a set of streamlined processes and systems must be established that can easily identify where personal information is stored, understand how this information is processed physically and electronically, who has access to this information, as well as for what purpose it is required.

This article must be read in conjunction with the POPI Act which can be downloaded from Act No. 4 of 2013 : Protection of Personal Information Act, 2013

Records Retention	POPIA requires that records be captured, kept and maintained: • Only those relevant to the purpose. • And only for the length of time for which they are required. • They need to be kept up to date. • Only used for the purpose for which they were gathered.

	This implies that the following records management aspects need to be considered. • A records retention schedule needs to be created.
Records disposal	• A disposal programme needs to be implemented and then rigidly followed. It is highly risky under POPIA to keep records and not destroy them when they have served their purpose.This does of course apply to all records and should not be limited to Personal Information records. • A key element of disposal is to ensure that duplicates are also destroyed as they are also Personal Information. A process of identifying and removing duplicates should be adopted. Duplicates could be in paper or electronic formats.
File Plan or Business Classification Scheme	• A structured classification scheme should be developed so that records can be easily identified, stored, retrieved and managed. This should be designed to cater for records on all formats and in all locations. This is essential if records are to be managed correctly in terms of POPIA.
Conditions for lawful processing of personal information	The POPI Act is a new all-inclusive piece of legislation that safeguards the integrity and sensitivity of private information. Companies are required to carefully manage the data capture and storage process of Personal Information within the lawful framework as set out in the Act. Below is the definition of Personal Information as stated in the POPI Act: ***"personal information*** *means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:* 1. *information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person.* 2. *information relating to the education or the medical, financial, criminal or employment history of the person.*

	3. *any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person.* 4. *the biometric information of the person.* 5. *the personal opinions, views or preferences of the person.* 6. *correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence.* 7. *the views or opinions of another individual about the person; and* 8. *the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information* about the person;" The Act provides 8 conditions under which Personal Information may legally be gathered and processed. This document must be read in conjunction with the POPI Act be found at http://www.justice.gov.za/legislation/acts/2013-004.pdf *A POPIA policies and procedures manual will be required. It is the duty of the Information Officer to ensure that these policies and procedures are followed.* One of the key aspects of any privacy law, and POPIA in particular, is that it describes the conditions for lawful processing. In other words, the conditions that need to be met when you manage personal information correctly. Meeting these conditions are mandatory if the organisation is seeking compliance to POPIA.
The 8 POPIA Conditions: **1. Accountability- Section 8**	The responsible party must ensure that the conditions and all the measures set out in the Act that give effect to such conditions, are complied with at the time of determining the purpose and means of the processing. Questions to ask: • **Who will be tasked with the responsibility of compliance in your organisation**? *This individual will be held liable for non-compliance in certain situations.*

	How will this individual ensure the organisation is POPI compliant? *Policies and Procedures* *Regular checks and audits*
2. Processing Limitation- section 9 to12	Personal information may only be processed in a fair and lawful manner and only with the consent of the data subject. Questions to ask: • **Was the personal information obtained directly from the Data Subject?** *One of the requirements of the Act is that any personal information must be obtained directly from the Data Subject.* • **Is the Data Subject aware that you have gathered his/her information and consented to the information being used?** *Consent from the Data Subject is essential before gathering or processing any personal information.* • **If the personal information has been gathered from a third party, has the Data Subject consented to this information being shared and used by you?** *This is a requirement.* • **Is the amount of information being gathered excessive?** *Only information that is required for the specific purpose for which it is gathered may be stored. You may collect more information than required for the intended purpose for future use if you obtain the necessary consent from the Data Subject (this is regarded as "Further Processing" in the Act.*
3. Purpose Specification - Section13 to 14	Personal information may only be processed for specific, explicitly defined and legitimate reasons. Questions to ask: • **For what specific, explicit and lawful purpose is the personal information being collected?** *This purpose must be documented and adhered to.* • **Is the Data Subject aware of the purpose for which the data has been collected?** *Data Subject has the right to know what information you have and for what purpose it was gathered.* • **Can you link all personal information collected to legitimate reasons for collecting?** *Personal information only to be gathered for specific, explicit and lawful purposes.*

	• **For what period may you retain specific personal information?** *Personal information may only be used for the specific purpose for which it was gathered and thereafter it must be destroyed.This procedure should be covered in the POPIA policies and procedures manual.* • **How will you keep track of when personal information must be destroyed**? *You will be required to account for what information you hold, for what purpose it was gathered and a date that that information must be destroyed.* **What process will be used to destroy Personal Information, in a manner that prevents its reconstruction, after you are no longer authorized to retain such records?** *This is an essential step in the process. This procedure should be covered in the POPIA policies and procedures manual*
4. Further Processing Limitation- Section 15	Personal information may not be processed for a secondary purpose unless that processing is compatible with the original purpose. Questions to ask: • **If you intend to reuse personal information, is it in accordance and compatible with the purpose for which it was collected?** *Should you want to use existing personal information for any other purpose other than what the information was gathered for, confirmation will be required from the Data Subject again*. • **Is the Data Subject aware of the continued use of their personal information?** *When gathering information, you have to advise the Data Subject what the information will be used for and for what period you will hold that information.*
5. Information Quality- Section 16	The responsible party must take reasonably steps to ensure that the personal information collected is complete, accurate, not misleading and updated where necessary. Questions to ask: • **How do you ensure that personal information is reliable and accurate at all times?** *By obtaining information directly from the data source, accuracy is more probable. It is always advisable to validate the personal information as it is being captured. If it is not possible for the data subject to input their own information, or if the information is captured from one*

	formalt to another (i.e. from a paper form to an IT system, then the information should be sent to the data subject for validation. • **What process do you have in place to allow Data Subjects to update their information or withdraw consent?** *When advising Data Subjects of the information you hold and for what purpose you hold it, they must be given details of how to update their information or withdraw consent. This procedure should be covered in the POPIA policies and procedures manual. It is advisable to develop procedures for automatically checking the accuracy of information on a regular basis, but sending a validation request to the data subjects.*
6. Openness- Sections 17 to 18	The data subject whose information you are collecting must be aware that you are collecting such personal information and for what purpose the information will be used. Questions to ask: • **How do you gather personal information from Data Subjects and what process do you have in place to get consent for collecting and using personal information?** *This is an important step and proof of consent is essential.* • **How do you inform the Data Subject of the purpose for which the information is being gathered?** *The Data Subject must be informed of how the data will be used at the time of gathering the information.* • **What evidence do you have that Data Subjects have consented to the collection of their personal information?** *Proof of consent must be retained to safeguard you against claims of misuse made by the Data Subject.* • **Does the Data Subject know who the responsible party is in your organization?** *When gathering information, Data Subjects must be given the details of the responsible person in your organization including contact details.* • **How do you inform the Data Subjects of their right to lodge a complaint with the Information Regulator?** *At the time that the personal information is gathered, the Data Subject must be advised of his/her rights to complain to the Information Regulator if misuse is suspected. The Information Regulator's information and contact details must be provided to the Data Subject.*

	• **Have you advised the Data Subject of his/her rights to access his/her information and to object to the processing of said information?** *This is a requirement.*
7. Security Safeguards- Sections 19 to 22	Personal information must be kept secure against the risk of loss, unlawful access, interference, modification, unauthorized destruction and disclosure. Questions to ask: • **What procedure do you have in place to identify any foreseeable internal and external risks to personal information?** *A safety and security risk assessment is required.* • **What processes do you have in place to prevent personal information from falling into unauthorized hands?** *Strict adherence to safety and security policies must be enforced. This procedure should be covered in the POPIA policies and procedures manual.* • **What procedure do you have in place to establish and maintain appropriate safeguards against the identified risks?** *The responsible person must enforce strict policies and procedures to safeguard personal information in your possession. This procedure should be covered in the POPIA policies and procedures manual.* • **How do you determine which employees are permitted access personal information and what information they are permitted to access?** *Strict policies and procedures are required regarding who has access, and how they gain access, to the personal information in your possession. This procedure should be covered in the POPIA policies and procedures manual.* • **What processes do you have in place to alert you when personal information is accessed or modified without authorization?** *This procedure should be covered in the POPIA policies and procedures manual.* • **What processes do you have in place to identify the source of a data breach and the procedure to follow to neutralize such breach?** *This procedure should be covered in the POPIA policies and procedures manual.* • **What process do you have in place to ensure that safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards?** *This procedure should be covered in the POPIA policies and procedures manual. It is the duty of the Responsible Person to ensure this process is followed.* • **What processes do you have in place to prevent the reoccurrence of a data breach?** *This procedure should be covered in the POPIA policies and procedures manual. It is the duty of the Responsible Person to ensure this process is followed.* • **What procedure is to be followed when sharing personal information with an external operator?** *A responsible party must, in terms of a written contract between the responsible*

	party and the operator, ensure that the operator establishes and maintains the required security measures. The operator must advise immediately if there is the possibility that personal data has been accessed or acquired by any unauthorized person. • **What procedure is in place to inform the Data Subject that their personal information has been compromised?** *The Data Subject must be advised via e-mail or in writing immediately if it is suspected that their personal information has been access by unauthorized persons. Sufficient information must be provided to allow the Data Subject to put measures in place to safeguard themselves against potential consequences of the security compromise. This procedure should be covered in the POPIA policies and procedures manual.* • **What procedure is in place to inform the Information Regulator of any security breach?** *The Information Regulator must be informed in the event of a security breach where personal information could be compromised. This procedure should be covered in the POPIA policies and procedures manual. It is the duty of the Responsible Person to ensure this process is followed.*
8.Data Subject Participation- **Section 23 to 35**	Data subjects may request whether their personal information is held, as well as the correction and/or deletion of any personal information held about them. Questions to ask: • **What are the Data Subject's rights regarding access to information being held by you?** *Data Subjects may request information from you on whether you are holding their personal information. This request may not be declined and may not be charged for. The full nature and details of the information being held must also be provided on request, but a charge may be levied for this information.* • **What processes do you have in place to ensure such a request from a Data Subject is adhered to?** *This procedure should be covered in the POPIA policies and procedures manual. It is the duty of the Responsible Person to ensure this process is followed.* • **What processes do you have in place to allow Data Subjects to correct personal information that you hold or withdraw consent to use such information?** *The Data Subject has the right to correct the personal information that you hold. They also have the right to withdraw consent at any time. This procedure*

	should be covered in the POPIA policies and procedures manual.
9.Transborder Information Flows-Section72 **<u>Transfer of Personal Information out of South Africa</u>**	The Act controls the transfer of personal information from South Africa to foreign countries and prohibits this unless: (section 71) • the person receiving the information is subject to similar laws. • the subject has agreed to the transfer of information. • such transfer is part of the performance of a contract which the subject is a party; or • transfer is for the benefit of the subject and it is not reasonably practicable to obtain their consent and that such consent would be likely to be given. (section72) ***Read in conjunction with the POPI Act which can be downloaded from Act No. 4 of 2013 : Protection of Personal Information Act, 2013***
<u>Offences, Penalties and Administrative Fines</u>	Sections 100 – 106 of the POPI Act deal with instances where parties would find themselves "guilty of an offense". The most relevant of these are: • Any person who hinders, obstructs, or unlawfully influences the Regulator. • A responsible party which fails to comply with an enforcement notice. • Offences by witnesses, for example, lying under oath or failing to attend hearings. • Unlawful Acts by responsible party in connection with account numbers. • Unlawful Acts by third parties in connection with account number. Section 107 of the Act details which penalties apply to respective offenses. For the more serious offences the maximum penalties are a R10 million fine or imprisonment for a period not exceeding 10 years or to both a fine and such imprisonment. For the less serious offences, for example, hindering an official in the execution of a search and seizure warrant the maximum penalty would be a fine or imprisonment for a period not exceeding 12 months, or to both a fine and such imprisonment.

	Failure to comply with the requirements of the POPI Act could have dire consequences. **This article must be read in conjunction with the POPI Act** which can be downloaded from Act No. 4 of 2013 : Protection of Personal Information Act, 2013
Disputes and Breaches	If someone is alleged to be in breach of the POPI Act, a complaint may be submitted to the Information Regulator. This complaint will be dealt with by an adjudicator. If a person is not happy with the determination of the adjudicator, they can still approach the Information Regulator for another ruling. Disputes and breaches are covered in complete detail in the Act and the Act should be consulted before drawing up Policies and Procedures to handle such matters. This article must be read in conjunction with the POPI Act which can be downloaded from Act No. 4 of 2013 : Protection of Personal Information Act, 2013
Direct Marketing	Section 69 of the Act outlaws direct marketing by means of any form of electronic communication unless the data subject has given their consent. Such an electronic communication obviously includes emails, SMS's and automatic calling machines. A subject can only be approached once to obtain such a consent. Once such consent is refused, it is refused forever. Slightly different rules apply if the subject is a customer. Here the customer's contact details must have been obtained in the context of the sale of a product or a service, the direct marketing by electronic communication can only relate to the suppliers own similar products or services, and the customer must have been given the right to opt out at the time that the information was collected and each time such a communication is sent. The Act covers Direct Marketing restrictions in full detail and should be consulted before any direct marketing campaign is considered. ***This article must be read in conjunction with the POPI Act which can be downloaded from Act No. 4 of 2013 : Protection of Personal Information Act, 2013***
Information Regulator	An Information Regulator has been appointed by the President on the recommendation of the National Assembly and is

	answerable to the National Assembly. There will be a large body of staff working under the Information Regulator. The Information Regulator's duties are varied and he/she has the power and authority to handle all matters relating to the POPIA Act. The Information Regulator must immediately be advised in the event of a breach which resulted in Personal Information falling into the wrong hands. ***This article must be read in conjunction with the POPI Act which can be downloaded from Act No. 4 of 2013 : Protection of Personal Information Act, 2013***
How Personal Information Needs to be Handled	Any organisation or person who keeps personal information must take steps to prevent the loss, damage, and unauthorized destruction of the personal information. In terms of Section 19, they are also required to prevent unlawful access to, or unlawful processing of this personal information. All risks have to be identified and then safeguards must be established and maintained against these risks. Regular verification that the safeguards are being effectively implemented is required. Safeguards are to be updated in response to any new risks or identified deficiencies in existing safeguards. Any person processing personal information on behalf of an employer must have the necessary authorization from the employer to do so. They must also treat the personal information as confidential and not share this information without the following the required processes. (section 20). The person must have a written contract with their employer in which they are specifically obliged to maintain the integrity and confidentiality of the personal information and to implement the established safeguards against identified risks. In terms of Section 21(2), the employee also has an obligation to notify their employer immediately if they believe that there has been a data breach. New employment contracts will be required for administrative staff, data capturers and for any employee who deals with personal information, to ensure that these requirements are met. In the event of a breach and personal information has been accessed or acquired by any unauthorized party the responsible party (Information Officer) is required to notify the Information Regulator, and the data subject needs to receive formal notification off this fact. The notification to the data subject must be provided with extreme haste and with sufficient information to allow the subject to protect themselves against the possible consequences of the personal information falling into the wrong hands. Everyone has the right to enquire as to whether somebody or an entity has their personal information on record. The enquiring

	party must provide proof of identity and the requested information must be provided to the data subject free of charge. To establish what this information consists of and whether this information has been disseminated to any third parties, payment may be required. Access to this information is also subject to the Promotion of Access to Information Act. Everyone has the right to have their personal information corrected or deleted if it is inaccurate, irrelevant, excessive, dated, misleading, or if it has been obtained unlawfully, or if the responsible party is no longer authorized to retain the information. **Special Personal Information** Section 26 of the POPI Act creates a special category of personal information called "special personal information". This relates to religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information. Also included in this category is information relating to the alleged commission of any offence or any proceedings in respect of any offence allegedly committed and the outcome of such proceedings. Failure to obtain consent makes processing this special personal information strictly prohibited, unless • it is necessary by law. • or is done for historical, statistical or research purposes. • or the information has been deliberately made public by the subject. There are limited exceptions to the prohibition against the processing of "special personal information". Details of such exceptions are set out in the Act. Special rules apply to the processing of personal information of children. (section35) These rules are set out in the Act. The Information Regulator has the power to grant exemptions to allow people to process personal information without complying with the Act if the public interest outweighs the subject's rights of privacy or where there is a clear benefit to the subject. Such exemptions may be granted if specific conditions have been met. Details of such exceptions are set out in the Act. ***This article must be read in conjunction with the POPI Act which can be downloaded from Act No. 4 of 2013 : Protection of Personal Information Act, 2013***
Data Subject Rights	**Data Subject Rights** Everyone has the right to be informed if someone is collecting their personal information, or if their personal information has been accessed by an unauthorized person. In addition, they have the right of access to their personal information and to

require that personal information be corrected or destroyed, or they may object to their personal information being processed.

The Act does not apply to personal information processed-

- during a personal or household activity,
- or where the processing authority is a public body involved in national security, defence, public safety, anti-money laundering,
- or the Cabinet or Executive Council of the Province
- or as part of a judicial function.

Personal information can only be processed: (Section 11)

- with the consent of the “data subject”; or
- if it is necessary for the conclusion or performance of a contract to which the “data subject” is a party; or
- if it is required by law; or
- if it protects a legitimate interest of the “data subject”; or
- if it is necessary to pursue your legitimate interests or the interest of a third party to whom the information is supplied.

Everyone has the right to object to having their personal information processed. They have the right to withdraw their consent, or object if they can show legitimate grounds for their objection.

A Responsible Party must collect personal information directly from the “data subject”, unless:

- this information is contained in some public record or has been deliberately published by the data subject.
- collecting the information from another source does not prejudice the subject.
- it is necessary for some public purpose; or to protect their own interests.
- obtaining the information directly from the subject would prejudice a lawful purpose or is not reasonably possible.

Personal Information may only be collected for a specific, explicitly defined and lawful purpose and the data subject must be aware of the purpose for which the information is being collected. (section13)

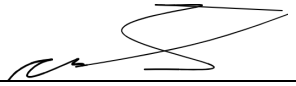
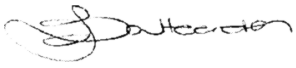
Once the Personal Information is no longer needed for the specific purpose for which it was gathered, it must be disposed of (or the data subject must be “de-identified”).

Personal Information may only be kept if it is allowed by law, or the information is needed to keep the record for lawful purpose or in accordance with the contract between the company and

	the data subject, or the data subject has consented to the data processor keeping the records. (section14) The company is entitled to keep records of personal information for historical, statistical or research purposes if it has been "de-identified" and safeguards have been established to prevent the records being used for any other purposes. Records must be destroyed in a way that prevents them from being reconstructed. Personal information may only be used for the purpose which the data was collected. (section15) Documentation relating to personal information and how it has been processed must be maintained as referred to in section 14 or 51 of the Promotion of Access to Information Act. When information is being collected, data subjects must be made aware of: (section 18) • the information that is being collected and if the information is not being collected from the subject, the subject must be made aware of the source from which the information is being collected. • the name and address of the person/organisation collecting the information. • the purpose of the collection of information • what period the information will be retained for and assurance given that it will be destroyed by given date. • whether the supply of the information by the subject is voluntary or mandatory. • the consequences of failure to provide the information. • whether the information is being collected in accordance with any law. • if it is intended for the information to leave the country and what level of protection will be afforded to the information after it has left South Africa. • who will be receiving the information? • that the data subject has access to the information and the right to rectify any details. • that the data subject has the right to object to the information being processed (if such right exists) • that the data subject has the right to lodge a complaint to the Information Regulator. The contact details of the Information Regulator must also be supplied. (section18) These requirements must be met before the information is collected directly from the subject, or soon as reasonably practicable. If additional information is collected from a subject for a different purpose, the same process must be followed.

	Contact details of The Information Regulator (South Africa): **JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001** P.O Box 31533, Braamfontein, Johannesburg, 2017 **Complaints** email: **complaints.IR@justice.gov.za**

APPROVAL

POSITION:	NAME:	SIGNATURE:	DATE:
Group CEO	S. Brachini		14/07/2021
Group CCO	L. Brachini		14/07/2021
Group CFO	B. Toker		07/07/2021
Group Compliance Officer	E. Whitford		07/07/2021
Group Operations and IT Executive	G. Billau		07/07/2021
Group Sales Executive	J. Dinis		06/07/2021
Group Financial Executive	M. Nel		06/07/2021
Supply Chain Manager	C. van Heerden		06/07/2021
Marketing Manager	J. Conradie		
Regional Sales Manager	B. Nogueira		06/07/2021
Corporate Sales Executive	S. Roux		06/07/2021

www.QuicklySign.com
Document Pack Id: lfvSdtJN4T0K8w17a7a68053a
Document Id: lfvSdtJN4T0K8w17a7a68053a_DXgGwv8cYE1JqU
Document 1 of 1
Document Name: 76b._ISO_9001_2015_Celcom Group Pty Ltd Popi - Popia Manual_ Celcom Group-_2021-06-29.pdf

Audit Trail

14/07/2021 12:51:52 SAST+0200: Status marked as complete.
14/07/2021 12:51:47 SAST+0200: Stefb@celcomgroup.co.za (Stefano Brachini) completed signing document 41.13.143.154
14/07/2021 12:51:17 SAST+0200: Stefb@celcomgroup.co.za (Stefano Brachini) accepted QuicklySign Terms and Conditions 41.13.143.154
14/07/2021 12:50:59 SAST+0200: Stefb@celcomgroup.co.za (Stefano Brachini) opened document 41.13.143.154
14/07/2021 12:50:58 SAST+0200: Stefb@celcomgroup.co.za (Stefano Brachini) clicked document link 41.13.143.154
14/07/2021 12:23:07 SAST+0200: Email has been received by stefb@celcomgroup.co.za mail server 167.89.84.21
14/07/2021 12:23:03 SAST+0200: Signature request sent to: Stefb@celcomgroup.co.za (Stefano Brachini)
14/07/2021 12:22:57 SAST+0200: lucab@celcomgroup.co.za (Luca Brachini) completed signing document 41.13.176.100
14/07/2021 12:22:25 SAST+0200: lucab@celcomgroup.co.za (Luca Brachini) accepted QuicklySign Terms and Conditions 41.13.176.100
14/07/2021 12:22:05 SAST+0200: lucab@celcomgroup.co.za (Luca Brachini) opened document via authenticated session 41.13.176.100
14/07/2021 08:24:38 SAST+0200: Email has been received by lucab@celcomgroup.co.za mail server 149.72.149.168
14/07/2021 08:24:34 SAST+0200: Signature request sent to: lucab@celcomgroup.co.za (Luca Brachini)
09/07/2021 08:24:39 SAST+0200: Email has been received by lucab@celcomgroup.co.za mail server 149.72.149.168
09/07/2021 08:24:34 SAST+0200: Signature request sent to: lucab@celcomgroup.co.za (Luca Brachini)
07/07/2021 08:24:29 SAST+0200: Email has been received by lucab@celcomgroup.co.za mail server 149.72.149.168
07/07/2021 08:24:23 SAST+0200: Signature request sent to: lucab@celcomgroup.co.za (Luca Brachini)
07/07/2021 08:24:17 SAST+0200: brett@celcomgroup.co.za (Brett Toker) completed signing document 105.27.143.114
07/07/2021 08:23:35 SAST+0200: brett@celcomgroup.co.za (Brett Toker) accepted QuicklySign Terms and Conditions 105.27.143.114
07/07/2021 08:23:19 SAST+0200: brett@celcomgroup.co.za (Brett Toker) opened document 105.27.143.114
07/07/2021 08:23:19 SAST+0200: brett@celcomgroup.co.za (Brett Toker) clicked document link 105.27.143.114
07/07/2021 08:09:59 SAST+0200: Email has been received by brett@celcomgroup.co.za mail server 167.89.84.21
07/07/2021 08:09:52 SAST+0200: Signature request sent to: brett@celcomgroup.co.za (Brett Toker)
07/07/2021 08:09:46 SAST+0200: lisa.whitford@celcomgroup.co.za (Lisa Whitford) completed signing document 102.182.173.193
07/07/2021 08:09:35 SAST+0200: lisa.whitford@celcomgroup.co.za (Lisa Whitford) accepted QuicklySign Terms and Conditions 102.182.173.193
07/07/2021 08:08:13 SAST+0200: lisa.whitford@celcomgroup.co.za (Lisa Whitford) opened document 102.182.173.193
07/07/2021 08:08:12 SAST+0200: lisa.whitford@celcomgroup.co.za (Lisa Whitford) clicked document link 102.182.173.193
07/07/2021 07:46:24 SAST+0200: Email has been received by lisa.whitford@celcomgroup.co.za mail server 167.89.84.21
07/07/2021 07:46:19 SAST+0200: Signature request sent to: lisa.whitford@celcomgroup.co.za (Lisa Whitford)
07/07/2021 07:46:12 SAST+0200: gregb@celcomgroup.co.za (Greg Billau) completed signing document 105.213.180.184
07/07/2021 07:45:51 SAST+0200: gregb@celcomgroup.co.za (Greg Billau) accepted QuicklySign Terms and Conditions 105.213.180.184
07/07/2021 07:45:38 SAST+0200: gregb@celcomgroup.co.za (Greg Billau) opened document 105.213.180.184
07/07/2021 07:45:38 SAST+0200: gregb@celcomgroup.co.za (Greg Billau) clicked document link 105.213.180.184
06/07/2021 15:09:25 SAST+0200: Email has been received by gregb@celcomgroup.co.za mail server 149.72.149.168
06/07/2021 15:09:20 SAST+0200: Signature request sent to: gregb@celcomgroup.co.za (Greg Billau)
06/07/2021 15:09:10 SAST+0200: john.dinis@celcomgroup.co.za (John Dinis) completed signing document 105.27.143.114
06/07/2021 15:08:45 SAST+0200: john.dinis@celcomgroup.co.za (John Dinis) accepted QuicklySign Terms and Conditions 105.27.143.114
06/07/2021 15:08:31 SAST+0200: john.dinis@celcomgroup.co.za (John Dinis) opened document 105.27.143.114
06/07/2021 15:08:30 SAST+0200: john.dinis@celcomgroup.co.za (John Dinis) clicked document link 105.27.143.114
06/07/2021 11:35:16 SAST+0200: Email has been received by john.dinis@celcomgroup.co.za mail server 168.245.102.10
06/07/2021 11:35:06 SAST+0200: Signature request sent to: john.dinis@celcomgroup.co.za (John Dinis)
06/07/2021 11:35:00 SAST+0200: melissa.nel@celcomgroup.co.za (Melissa Nel) completed signing document 105.27.143.114
06/07/2021 11:34:24 SAST+0200: melissa.nel@celcomgroup.co.za (Melissa Nel) accepted QuicklySign Terms and Conditions 105.27.143.114
06/07/2021 11:33:54 SAST+0200: melissa.nel@celcomgroup.co.za (Melissa Nel) opened document via authenticated session 105.27.143.114
06/07/2021 11:30:06 SAST+0200: Email has been received by melissa.nel@celcomgroup.co.za mail server 167.89.84.21
06/07/2021 11:30:01 SAST+0200: Signature request sent to: melissa.nel@celcomgroup.co.za (Melissa Nel)

06/07/2021 11:29:54 SAST+0200: cindy.vanheerden@celcom.co.za (Cindy Van Heerden) completed signing document 105.27.143.114
06/07/2021 11:29:36 SAST+0200: cindy.vanheerden@celcom.co.za (Cindy Van Heerden) accepted QuicklySign Terms and Conditions 105.27.143.114
06/07/2021 11:28:35 SAST+0200: cindy.vanheerden@celcom.co.za (Cindy Van Heerden) opened document 105.27.143.114
06/07/2021 11:28:34 SAST+0200: cindy.vanheerden@celcom.co.za (Cindy Van Heerden) clicked document link 105.27.143.114
06/07/2021 11:26:40 SAST+0200: Email has been received by cindy.vanheerden@celcom.co.za mail server 167.89.84.21
06/07/2021 11:26:35 SAST+0200: Signature request sent to: cindy.vanheerden@celcom.co.za (Cindy Van Heerden)
06/07/2021 11:26:28 SAST+0200: justin.conradie@celcomgroup.co.za (Justine Conradie) completed signing document 102.182.103.72
06/07/2021 11:26:06 SAST+0200: justin.conradie@celcomgroup.co.za (Justine Conradie) accepted QuicklySign Terms and Conditions 102.182.103.72
06/07/2021 11:25:26 SAST+0200: justin.conradie@celcomgroup.co.za (Justine Conradie) opened document 102.182.103.72
06/07/2021 11:25:26 SAST+0200: justin.conradie@celcomgroup.co.za (Justine Conradie) clicked document link 102.182.103.72
06/07/2021 09:46:12 SAST+0200: Email has been received by justin.conradie@celcomgroup.co.za mail server 149.72.149.195
06/07/2021 09:46:07 SAST+0200: Signature request sent to: justin.conradie@celcomgroup.co.za (Justine Conradie)
06/07/2021 09:46:01 SAST+0200: brunon@celcom.co.za (Bruno Nogueira) completed signing document 102.165.252.79
06/07/2021 09:45:41 SAST+0200: brunon@celcom.co.za (Bruno Nogueira) opened document via authenticated session 102.165.252.79
06/07/2021 09:40:03 SAST+0200: Email has been received by brunon@celcom.co.za mail server 149.72.251.1
06/07/2021 09:39:57 SAST+0200: Signature request sent to: brunon@celcom.co.za (Bruno Nogueira)
06/07/2021 09:39:51 SAST+0200: siegfriedr@celcom.co.za (Siegfried Roux) completed signing document 105.242.60.254
06/07/2021 09:39:23 SAST+0200: siegfriedr@celcom.co.za (Siegfried Roux) accepted QuicklySign Terms and Conditions 105.242.60.254
06/07/2021 09:38:58 SAST+0200: Email has been received by siegfriedr@celcom.co.za mail server 149.72.149.195
06/07/2021 09:38:53 SAST+0200: Signature request sent to: siegfriedr@celcom.co.za (Siegfried Roux)
06/07/2021 09:38:37 SAST+0200: siegfriedr@celcom.co.za (Siegfried Roux) opened document 105.242.60.254
06/07/2021 09:38:37 SAST+0200: siegfriedr@celcom.co.za (Siegfried Roux) clicked document link 105.242.60.254
06/07/2021 09:38:16 SAST+0200: Email has been received by siegfriedr@celcom.co.za mail server 149.72.149.195
06/07/2021 09:38:11 SAST+0200: Signature request sent to: siegfriedr@celcom.co.za (Siegfried Roux)
06/07/2021 09:38:03 SAST+0200: lisa.whitford@celcomgroup.co.za (Lisa Whitford) changed the status to:awaiting_signatures 105.27.143.114
06/07/2021 08:40:57 SAST+0200: lisa.whitford@celcomgroup.co.za (Lisa Whitford) changed the status to:setup 105.27.143.114
06/07/2021 08:40:48 SAST+0200: brunon@celcom.co.za (Bruno Nogueira) accepted QuicklySign Terms and Conditions 102.165.252.79
06/07/2021 08:40:32 SAST+0200: brunon@celcom.co.za (Bruno Nogueira) opened document 102.165.252.79
06/07/2021 08:40:32 SAST+0200: brunon@celcom.co.za (Bruno Nogueira) clicked document link 102.165.252.79
06/07/2021 08:31:28 SAST+0200: Email has been received by brunon@celcom.co.za mail server 149.72.251.1
06/07/2021 08:31:23 SAST+0200: Signature request sent to: brunon@celcom.co.za (Bruno Nogueira)
06/07/2021 08:31:17 SAST+0200: siegfriedr@celcom.co.za (Siegfried Roux) completed signing document 41.13.212.126
06/07/2021 08:30:30 SAST+0200: siegfriedr@celcom.co.za (Siegfried Roux) accepted QuicklySign Terms and Conditions 41.13.212.126
06/07/2021 08:26:55 SAST+0200: siegfriedr@celcom.co.za (Siegfried Roux) opened document 41.13.212.126
06/07/2021 08:26:54 SAST+0200: siegfriedr@celcom.co.za (Siegfried Roux) clicked document link 41.13.212.126
06/07/2021 08:24:53 SAST+0200: Email has been received by siegfriedr@celcom.co.za mail server 149.72.251.1
06/07/2021 08:24:48 SAST+0200: Signature request sent to: siegfriedr@celcom.co.za (Siegfried Roux)
06/07/2021 08:24:39 SAST+0200: lisa.whitford@celcomgroup.co.za (Lisa Whitford) changed the status to:awaiting_signatures 105.27.143.114
06/07/2021 08:01:20 SAST+0200: lisa.whitford@celcomgroup.co.za (Lisa Whitford) uploaded document 105.27.143.114

Supporting documentation

Supporting documents that were uploaded, as part of the signing process, can be found on document page online.

Online verification

This document can be verified online here
https://app.quicklysign.com/verify_document/lfvSdtJN4T0K8w17a7a68053a_DXgGwv8cYE1JqU