Privacy Policy

Ref No.: 45 0092 6504

Rev: 00

DOCUMENT HISTORY	
Effective Date	01 January 2024

APPROVALS			
STATUS	**TITLE**	**NAME**	**SIGNATURE**
Prepared	Network Manager	Mark Higgins	
Reviewed	ICT Manager	Khule Dlamini	Khule Dlamini (Jun 10, 2024 08:55 GMT+2)
Approved	Human Capital Executive	Ahmed Ashruf	Ahmed Ashruf (Jul 11, 2024 15:53 GMT+2)

Contents

1 INTRODUCTION

- Every person has rights with regard to how their personal information is handled and protected. To conduct its business and provide its services, the company may collect, store and process personal information about:
  1..1. employees.
  1..2. customers.
  1..3. consumers.
  1..4. service providers / suppliers; and
  1..5. business contacts.
  1..6. Partners
  1..7. Community
- Conlog recognises the need to treat this information in an appropriate and lawful manner. Conlog is committed to complying with its obligations in this regard in respect of all personal information it handles, in a manner which maintains the confidence of Conlog's customers, service providers / suppliers, business contacts and employees.
- The Protection of Personal Information Act no. 4 of 2013 (**"POPIA"**) and regulations (2018) relate to identifiable, living, natural persons and identifiable, existing, juristic persons. The European Union General Data Protection Regulation (**"GDPR"**) only relates to the information of European Citizens (natural persons). Additional privacy legislation may also be applicable should Conlog also conduct business in another country.
- The types of information that Conlog may be required to handle include details of current, past, and prospective employees, service providers / suppliers, customers, consumers, and other business contacts that Conlog may engage. The information would typically include names, addresses, email addresses, dates of birth, identity / passport numbers, phone numbers, private and confidential information and, potentially, special personal information. In addition, Conlog may occasionally be required to collect and use certain additional types of personal information to comply with the requirements of the law.
- The information may be stored on paper, electronically or by other media and is subject to certain legal safeguards specified in POPIA and GDPR, and potentially other applicable acts and regulations. The provisions of POPIA and GDPR impose restrictions on how Conlog may collect and process the personal information in question.
- This Information Privacy Policy ("**Policy**") may be amended from time to time. Any breach of this policy will be taken seriously by Conlog.

2 PURPOSE

- This policy sets out Conlog's general rules and the important legal conditions that must be satisfied in relation to the collecting, obtaining, handling, processing, storage, transportation, and destruction of identifiable personal and special personal

information.

- This policy also describes the privacy compliance framework and information governance of Conlog in detail.

3 SCOPE

This policy is applicable to all (i) employees, (ii) contractors, (iii) visitors, and / or (iv) other persons authorised to access and use Conlog's on-premises and online systems ("**Users**").

4 ROLES & RESPONSIBILITIES

The appointed Information Officer and his/her assistant are responsible for the implementation and monitoring of this policy.

4.1 As a Conlog employee, contractor, service provider or business partner, the onus lies on you to learn, understand and adhere to the following:

4.1.1.1 what actions are specifically required or prohibited by POPIA, PAIA, GDPR; and

4.1.1.2 to recognise areas where POPIA, PAIA and GDPR problems may arise and seek guidance from the relevant manager, who may in turn refer matters to the Deputy Chief Information Officer and the Chief Information Officer.

4.1.1.3 You acknowledge that periodic reviews can be conducted to ensure and monitor your adherence to this policy.

4.2 The provisions of POPIA, PAIA and GDPR can be complex, and you are encouraged to seek advice if you have any questions. To this end, Conlog's Information Officers will assist you on matters relating to the interpretation of POPIA.

4.3 Senior management is expected to use all reasonable efforts to ensure awareness of, and compliance with, this policy. Such reasonable efforts include, but are not limited to, frequent communications with employees and staff members.

4.4 Conlog Staff are expected to:

4.4.1.1 read and understand this policy.

4.4.1.2 acquaint themselves with, and abide by, the conditions.

4.4.1.3 understand how to conform to the expected standard during the lifecycle, and in particular, the expected standard in relation to the safeguarding of personal information.

4.4.1.4 understand what is meant by Special Personal Information (discussed in more detail below) and know how to handle such information.

4.4.1.5 not to jeopardize a Data Subject's privacy; and

4.4.1.6 not risk a contravention of POPIA, PAIA and GDPR.

5 REFERENCES

Reference Documents

	Document	Document Number
1.	Enterprise Cyber Security Policy	45 0092 6001
2.	Services Team Change Control Process & Procedure	11 0085 5000 R02
3.	ICT Continuity Management Policy	45 0092 6503

4.	Disaster Recovery Plan (DRP) document.	20 0014 5014
5.	Data & Information Management policy	TBA
6.	Publica Access to Information Act (PAIA)	N/A
7.	General Data Protection Regulation (GDPR)	N/A

Applicable Forms

	Form	Form Number
1.	Form 1: Objection to the Processing of Personal Information.	
2.	Form 2: Request for Correction or Deletion of Personal Information or Destroying or Deletion of Record of Personal Information.	
3.	Form 4: Application for the Consent of a Data Subject for the Processing of Personal Information for the Purpose of Direct Marketing	

Applicable Systems

	System
1.	• Sage 300 People (VIP) • Fresh Service (ICT Service Desk) • Fresh Service (Customer Support Centre) • SAP R/3 • SAP S/4 HANA • SAP Successfactors • SHEQsys • Salesforce • Conlog Rewards System

6 ABBREVIATIONS AND DEFINITIONS

Abbreviations

Abbreviation	Description
POPIA	Project of Personal Information Act
PAIA	Public Access to Information Act
PCC	Privacy Champions Committee
PDIA	Data Privacy Impact Assessment

Definitions

6.1 POPIA Definitions

Term	Meaning
“Data subject”	means all living, identifiable natural or juristic persons about whom

	Conlog holds personal information or special personal information;
"operator"	means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.
"Personal information"	means information relating to an identifiable, living, natural or juristic person, including (i) factual information, such as identity and passport numbers, names, addresses, phone numbers, email addresses and the like, or (ii) opinions regarding a data subject, such as a performance appraisal;
"processing"	means any operation or activity, whether or not by automatic means, concerning personal information, including the: • collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use of personal information. • dissemination of such information by means of transmission, distribution or making available in any other form; or • merging, linking, as well as restriction, degradation, erasure, or destruction of information;
"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; and
"Special personal information"	means more sensitive information about an individual that pertains to racial or ethnic origins, political, religious or philosophical beliefs, health or sexual life, trade union membership or political persuasion, biometric information or criminal behaviour (to the extent that such criminal behaviour relates to the alleged commission by a data subject of an offence or any proceedings in respect of any offence allegedly committed by a data subject, which can only be processed under strict conditions and will usually require the express written consent of the data subject concerned.

6.2 GDPR Definitions

Term	**Meaning**
"controller"	means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
"Personal data"	means any information relating to an identified or identifiable natural person directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or

	to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; and
"processing"	means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; and
(''**data subject**'').	An identifiable natural person is one who can be identified,
(processor"	means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

7 POLICY STATEMENTS

8 PRIVACY COMPLIANCE FRAMEWORK

8.1 To ensure compliance with the requirements of relevant privacy legislation such as POPIA and GDPR, Conlog has established a compliance framework with the following focus areas that must be addressed:

8.1.1 governance.

8.1.2 people.

8.1.3 process; and

8.1.4 technology.

8.2 Focus on governance.

8.3 Conlog undertakes to take accountability for its actions by implementing good corporate governance.

8.4 The focus on governance means that Conlog will establish a Privacy Committee Champions **(PCC)** and other structures to ensure that data protection compliance is an ongoing process and that continued management of information processes takes place.

8.5 Focus on process.

8.6 Conlog undertakes to implement processes to ensure that personal information is processed in line with relevant legislation.

8.7 This will include performing a Data Privacy Impact Assessment ("**DPIA**"), as required by regulations promulgated under POPIA, and also developing, implementing the necessary policies and procedures as well as other control measures to ensure compliance with the relevant privacy legislation.

8.8 Focus on people.

8.9 Most information security breaches involve people in one way or another. Conlog undertakes to ensure that Users are made aware of their responsibilities in relation to processing personal information.

8.10 Users must undergo privacy and information security training at least annually and all new employees must be appropriately trained within 3 (Three) months of commencing employment with Conlog.

8.11 Focus on technology.

8.12 Conlog undertakes to implement technology with appropriate security safeguards. The reference to "technology" includes software, hardware, and data specific requirements. Appropriate security technological safeguards must be in place where personal information is processed, stored, and destroyed. Conlog undertakes to appoint a specialist manager in information & communication technology ("**ICT**") to set up and manage Conlog's technology. This will be a combination of in-house employees and outsourcing to compliant third parties.

9 INFORMATION GOVERNANCE

9.1 INFORMATION OFFICER

9.1.1.1 The responsibilities of the information officer designated in terms of the POPIA include:

9.1.1.2 the encouragement of compliance, such as awareness and training, by Conlog, taking into consideration all of the conditions for the lawful processing of personal information.

9.1.1.3 ensuring compliance by Conlog with the provisions of POPIA.

9.1.1.4 dealing with requests made to Conlog in terms of POPIA, such as requests made from data subjects to update or view their personal information.

9.1.1.5 working with the information regulator ("Regulator") in relation to investigations; and

9.1.1.6 the designation and delegation of relevant duties to Champions appointed by Conlog.

9.1.1.7 The responsibilities of the information officer have been expanded upon in the regulations promulgated under POPIA on 14 December 2018. In this regard, the information officer must ensure that:

9.1.1.8 a compliance framework is developed, implemented, monitored and maintained.

9.1.1.9 a DPIA is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information.

9.1.1.10 a manual is developed, monitored, maintained, and made available as prescribed in sections 14 and 51 of the Promotion of Access to Information Act 2 of 2000.

9.1.1.11 internal measures are developed, together with adequate systems, to process requests for information or access thereto; and

9.1.1.12 internal awareness sessions are conducted regarding (i) the provisions of POPIA, (ii) regulations promulgated in terms of POPIA, (iii) relevant industry codes of conduct, or (iv) information obtained from the Regulator.

9.2 PRIVACY CHAMPION

9.2.1.1 The role of the departmental privacy champion (PC) will include:

9.2.1.1.1 Acquiring knowledge about Data Protection concepts and Conlog's Privacy Program "in the trenches" and share it with colleagues.

9.2.1.1.2 Promoting the Privacy Program within own department and cross-company

9.2.1.1.3 Identifying issues and risks within own department

9.2.1.1.4 Identifying potential areas of resistance to the changes associated with POPIA/GDPR

9.2.1.1.5 Becoming a "go-to person" during the program and post implementation of key policies and/or procedures, etc.

9.2.1.2 The responsibilities of a Privacy champion will include:

9.2.1.2.1 Act as a role model for privacy concepts and tasks.

9.2.1.2.2 Understanding the key impacts of the POPIA/GDPR Conlog and specifically to own department

9.2.1.2.3 Understanding the key Privacy Program deliverables, milestones and timeline

9.2.1.2.4 Attending program meetings when required

9.2.1.2.5 Assisting with cascading program communications

9.2.1.2.6 Reviewing relevant key deliverables and provide feedback.

9.2.1.2.7 Attending train-the-trainer sessions

9.2.1.2.8 Providing ongoing support to colleagues in own department during the program

9.2.1.2.9 Introducing new colleagues to required POPIA/GDPR education and training.

10 PRIVACY CHAMPIONS COMMITTEE (PCC) RESPONSIBILITES

10.1 **Strategic**: The oversight of the full information lifecycle for both structured and unstructured information, including:

10.1.1.1 endorsement of information policies, principles, and procedures in relation to information management.

10.1.1.2 assisting with ensuring compliance with the provisions of POPIA and GDPR, where applicable, which include the following:

10.1.1.2.1 The security and integrity of data/information held by, or on behalf of Conlog.

10.1.1.2.2 The dissemination of Conlog's data/information to third parties.

10.1.1.2.3 Information and data confidentiality and availability.

10.1.1.2.4 Information and data quality, including completeness, accuracy and ensuring that information is up to date.

10.1.1.2.5 Information sharing arrangements with other parties.

10.1.1.2.6 Retention and destruction of information practices.

10.1.1.2.7 Document management, including the digitisation of documents; and

10.1.1.3 Discussing and identifying the areas where consent will be needed for the processing of personal information.

10.1.1.4 Assisting with the integration of people, technologies, information, and processes across Conlog.

10.1.1.5 Identifying and assessing the information risks and provide input to Conlog's enterprise-wide risk management process.

10.1.1.6 Ensuring that there is proactive monitoring of data/information breach incidents and review the response to these incidents.

10.1.1.7 Reviewing and provide oversight to ensure that the information architecture supports confidentiality, integrity, and availability of information.

10.1.1.8 Endorsing information-related strategies and roadmaps.

10.1.1.9 Prioritising information-related initiatives.

10.1.1.9.1 Establishing information-related metrics and oversight of results.

10.1.1.9.2 Directing efforts to resolve issues in relation to information management.

10.1.1.9.3 Assisting with advice on the leverage of information to sustain and enhance Conlog's intellectual capital; and

10.1.1.9.4 Reviewing and assessing the actions taken to monitor the effectiveness of information management and how the outcomes were addressed.

10.2 **Operational**: The PCC will:

10.2.1.1.1 Establish structures needed to support information governance in Conlog.

10.2.1.1.2 Delegate authorities for the implementation of decisions.

10.2.1.1.3 Co-ordinate information management responsibilities across Conlog to ensure complete coverage of the information lifecycle.

10.2.1.1.4 Make the Users aware of the PCC and its roles and responsibilities.

10.2.1.1.5 Promote good information management practices so they can be notified of issues relating to their domain; and

10.2.1.1.6 Train and mentor teams to enable them to fulfil their roles.

11 INFORMATION PROCESSING PRINCIPLES

11.1 **POPIA**: Conlog fully supports and complies with the 8 (Eight) protection principles of POPIA which are summarised below:

11.1.1.1 **Accountability**: a responsible party must ensure that the information processing principles are complied with.

11.1.1.2 **Processing limitation**: personal information must be processed lawfully and in a reasonable manner.

11.1.1.3 **Purpose specification**: personal information must be obtained/processed for specific lawful purposes.

11.1.1.4 **Further processing limitation**: further processing of personal information must be in accordance or compatible with the purpose/s for which it was originally collected.

11.1.1.5 **Information quality**: personal information must be complete, accurate, not misleading and kept up to date.

11.1.1.6 **Openness**: personal information may only be processed by a responsible party who has taken reasonable steps to notify the data subject.

11.1.1.7 **Security safeguards**: personal information must be kept secure, and its confidentiality and integrity must be maintained; and

11.1.1.8 **Data subject participation**: a data subject has the right to request the responsible party to confirm, free of charge, whether or not the responsible party holds personal information, together with a description of the personal information held by such responsible party.

12 ACCOUNTABILITY

12.1 **The** provisions of POPIA are intended not to prevent the processing of personal information, but to make sure that a responsible party ensures that the information processing principles as set out in POPIA, and all the measures that give effect to the principles, are complied with.

12.2 The data subject must be told the identity of the responsible party (in this case, Conlog) and the purpose for which personal information is to be processed by Conlog.

12.3 This Policy, developed by Conlog to protect privacy, is available at Conlog premises and is also accessible online at Conlog's website and Shared Server. This policy outlines Conlog's commitment to privacy.

13 PROCESSING LIMITATION

13.1 For personal information to be processed lawfully, certain conditions have to be met. These may include, amongst other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the responsible party or the party to whom the personal information is disclosed. When special personal information is being processed, in most cases the data subject's explicit consent to the processing of such special personal information will be required.

13.2 A responsible party must collect personal information directly from the data subject unless (i) information is in a public record, (ii) the data subject has consented, (iii) the collection of personal information does not prejudice the legitimate interest of the data subject, or (iv) collection is necessary to comply with, or to avoid prejudice with or to the maintenance of, laws; to enforce legislation concerning the collection of revenue; for purposes of proceedings in a court; or in the interest of national security.

13.3 Where Conlog processes personal information as a responsible party, the data subject should be informed of this fact. The data subject should also be informed for what purpose the personal information is being processed by Conlog, and where or to whom such personal information may be disclosed or transferred. Conlog has drafted a “Terms of Use” document which can be found online at Conlog’s website, which explicitly outlines how and in what circumstances Conlog may use a person’s information.

14 PURPOSE SPECIFICATION

14.1 Personal information may only be processed for a specific and lawful purpose, or for any other purpose specifically permitted by POPIA, and steps must be taken to ensure that the data subject is aware of the purpose of the collection of the personal information. Conlog undertakes not to (i)collect personal information for one purpose and then use the personal information for another purpose, or (ii) retain personal information for any longer than is necessary for achieving the purpose for which the information was collected.

14.2 Personal information should only be collected to the extent that it is required for the specific purpose communicated to the data subject. Any personal information which is not necessary for that purpose should and will not be collected by Conlog.

14.3 If it becomes necessary to change the purpose for which the personal information is processed, the data subject will be informed of the new purpose before any processing occurs. Any employee personal information collected by Conlog will be used for ordinary human resources purposes. Where there is a need to collect employee personal information for any other purpose, the Company will notify the employee in question of this and, where it is appropriate and practicable, Conlog will get the employee’s consent prior to such processing.

14.4 Where Conlog collects personal information directly from a data subject, the personal information collected and processed by Conlog, such as identity number, proof of address and the like, will only be used for the required purpose.

15 FURTHER PROCESSING LIMITATION

15.1 Personal information should not be kept longer than is necessary for the purpose for which it was collected. For guidance in relation to a particular personal information retention period, a User should contact Conlog. Conlog has various legal obligations to keep certain personal information of Users for a specified period of time. In addition, Conlog may need to retain personal information for a period of time to protect its legitimate commercial and other interests.

15.2 Conlog will not use any personal information for any purpose other than that for which it received the information in the first place, unless any further processing of such information is compatible with the original purposes for which the information was collected.

16 INFORMATION QUALITY

16.1 Personal information must be complete, accurate, and kept up to date. Personal information which is incorrect, or misleading is not accurate, and steps will be taken to check the accuracy of any personal information at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date personal information will be destroyed. Employees should ensure that they notify their manager / Human Capital of any relevant changes to their personal information so that it can be updated and maintained accurately.

16.2 All personal information which is in paper form should be destroyed only by shredding. If the personal information is held electronically, Conlog must ensure that a reputable service provider destroys the personal information so that there is no future record of the information and Conlog must obtain an undertaking from the applicable service provider in this regard.

17 OPENNESS

17.1 Personal information may only be processed by Conlog if Conlog has notified the data subject that Conlog has obtained the information from legitimate sources.

17.2 In cases where Conlog works directly with a data subject, Conlog will take reasonable, practicable steps to ensure that the data subject is aware of the following:

17.2.1.1 What information is being collected and, where it is not collected from the data subject, the source of the information.

17.2.1.2 The full name and addresses of Conlog.

17.2.1.3 The purpose for which the information is being collected.

17.2.1.4 Whether supplying the personal information to Conlog is voluntary or mandatory.

17.2.1.5 The consequences of failure to provide the information.

17.2.1.6 The applicable law authorising or requiring the collection of the information.

17.2.1.7 The right to lodge a complaint against Conlog, the Regulator; and

17.2.1.8 Any further relevant information, such as recipient or category of recipients of information, nature of information, existence of the right of access and the right to rectify information collection.

18 SECURITY SAFEGUARDS

18.1 Conlog and its employees must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal information, and against the accidental loss of, or damage to, personal information.

18.2 Conlog will put in place procedures and technologies to maintain the security of all personal information. Personal Information may only be transferred to an operator if the operator has agreed to comply with those procedures and policies or has adequate security measures in place.

18.3 Users may refer to Conlog's information security and related policies for further information concerning Conlog’s security safeguards.

18.4 The following principles must be maintained by Conlog:

18.4.1.1 **Confidentiality:** that only people who are authorised to use the personal information in question can access it. Conlog will ensure that only authorised persons have access to an employee’s personnel file and any other personal or special information held by Conlog. Employees are required to maintain the confidentiality of any personal information and / or special personal information that they have access to.

18.4.1.2 **Integrity:** that proper security safeguards are in place to ensure the maintenance and assurance, of the accuracy and consistency of information / data over its entire life cycle.

18.4.1.3 **Availability**: that authorised users should be able to access the personal information if they need it for an authorised purpose.

18.4.1.3.1 **Examples** of security procedures at Conlog include:

18.4.1.3.1.1 *Secure lockable desks and Cupboards* – desks and cupboards must be kept locked if they hold confidential personal identifiable information of any kind.

18.4.1.3.1.2 Methods of Disposal – paper documents must be shredded. CD-ROMs and USB keys should be physically destroyed when they are no longer required.

18.4.1.3.1.3 *Equipment* – data users must ensure that individual computer monitors do not show confidential information to passers-by and that they log off from their computer when it is left unattended; and

18.4.1.3.1.4 User Management – any access to Conlog database is logged by Conlog through a username and password system. Any changes / updates / uploads to the system are constantly tracked.

18.5 Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, Conlog or any third party processing personal information under the authority of Conlog, must notify the Regulator and the data subject as soon as is reasonably possible, taking into consideration the time that is taken by Conlog to determine the scope of the breach and to restore the integrity of its information systems.

18.6 Any notification to a data subject must be in writing and communicated to the data subject in at least one of the following ways:

18.6.1.1 Mailed to the data subjects last known physical or postal address.

18.6.1.2 Sent by email to the data subjects last known email address.

18.6.1.3 Placed in a prominent position on the website of Conlog.

18.6.1.4 Published in the news media; or

18.6.1.5 As directed by the Regulator.

18.7 The notification referred to above must provide sufficient information to all the affected data subjects to take protective measures against the potential consequences of the security compromise including:

18.8 a description of the possible consequences of the security compromise.

18.9 a description of the measures that Conlog intends to take or has taken to address the security compromise.

18.10 a recommendation regarding the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and

18.11 if known to Conlog, the identity of the unauthorised person who may have accessed or acquired the personal information in question.

19 DATA SUBJECT PARTICIPATION

19.1 A formal request from a data subject for information that Conlog holds about them must be made in writing, accompanied with adequate proof of identification (in most instances, a certified copy of the individual's identity document or passport and proof of residence will be sufficient).

19.2 Any employees who receive a written request in respect of data held by Conlog must forward it to the information officer immediately.

19.3 Any individual requesting personal information that may be held by Conlog will be referred by the relevant employee to whom the request was made to the information officer, who will process the request. The information officer will either process the request directly or will direct such employee to request a certified copy of the individual's identity document or passport as well as proof of address. Once this is received, the employee will then be authorised to release the personal information to the individual. The employee must:

19.3.1.1 Record the request in the request register / system; and

19.3.1.2 Safely store the certified copy of the identity document and passport either in a file in a locked cupboard (if in paper format) or online in an encrypted folder which cannot be accessed by unauthorised personnel. Storage of these documents should be kept for 1 (one) year, after which they must be properly destroyed.

19.3.1.3 Any employee dealing with telephonic enquiries from data subjects should guard against disclosing any personal information held by Conlog over the phone. In particular, the employee must:

19.3.1.4 Check the identity of the caller to ensure that information will only be given to a person who is entitled to that information – this can be accomplished by confirming: identity number, date of birth, address, cell phone number and the like.

19.3.1.5 Request that the caller put their request in writing if the employee is not completely sure about the identity of the caller and in circumstances where the identity of the caller cannot be verified. In these circumstances, the employee should also request that a certified copy of the identity document / passport of the individual is provided before information is released.

19.3.1.6 Refer the request to their manager for assistance in difficult situations. No employee should feel forced to disclose personal information; and

19.3.1.7 Where a request has been made in terms of this section, and personal information is communicated to the data subject, the data subject must be advised of their right to request the correction of the information.

19.3.1.8 The data subject may request that Conlog correct or delete personal information, which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully, or to destroy such record of personal information. If such a request is made, Conlog must send this request to the appropriate party within Conlog who should then correct the information, destroy, or delete it, and provide the data subject with credible evidence that this has been done.

20 GENERAL DATA PROTECTION REGULATION (GDPR)

20.1 The company fully supports and complies with the 6 (Six) protection principles of the GDPR which are summarised below:

20.2 **Lawfulness, fairness, and transparency**: The personal information of the European citizens will be processed lawfully, fairly and in a transparent manner in relation to the data subject.

20.3 **Purpose limitation:** The personal information of the European citizens will be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for achieving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purpose.

20.4 **Data Minimisation**: The personal information of the European citizens will be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

20.5 **Accuracy**: The personal information of the European citizens will be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purpose for which it is processed, is erased, or rectified without delay.

20.6 **Storage Limitation**: The personal information of the European citizens will be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1), subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.

20.7 **Integrity and Confidentiality**: The personal information of the European citizens will be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

21 REVIEW

21.1 Conlog will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives on at least an annual basis and more frequently if required, considering changes in the law and organisational or security changes.

21.2 A compulsory review of this policy will be conducted every three (3) years or as changes occur in the course of business.

22 NON-COMPLIANCE

22.1 Non-compliance to this policy constitutes misconduct and shall be dealt with in accordance with Conlog Employee Relations policies.

23 REVISION CONTROL

Revision	Date	Compiler	Change
00	April 2024	K. Dlamini	New Issue

24 DOCUMENT DISTRIBUTION LIST

Distribution group	Yes	No	Comments
Conlog All	☒	☐	
Division All	☐	☐	
Department all	☐	☐	
Department	☐	☐	
Specific employee group	☐	☐	
Other	☐	☐	