concor	Document Title	PROTECTION OF PERSONAL INFORMATION POLICY (POPI)
	Document Number	COY-IMS-LGL-POL-004
	Document Revision	1
	Function	Governance, Risk and Compliance
	Date Approved	2022/08/25
	Document Owner	Thirosha Govender
	Accountable Director	Juanita Putter
	Number of Pages	10

PROTECTION OF PERSONAL INFORMATION POLICY

Revision	Amendment Description	Approval	Date
0	Original	Nosipho Maphumulo	2021/05/31
1	General review	Junita Putter	2022/08/25

1. PURPOSE

This Policy is implemented in compliance with the provisions of the *Protection of Personal Information* Act 4 of 2013 and its Regulations in order to give effect to the Constitutional right to privacy.

This Policy will regulate and protect *Personal Information* and the rights and interests of all *Data Subjects* who provide *Personal Information* to the Company.

2. SCOPE

This Policy applies to all *Personal Information* processed by the Company and any Group Company in the exercise of its functions and obligations as a business entity, including the *Personal Information* of the Company's customers, employees and suppliers.

3. RESPONSIBILITY

The Concor Group management is responsible for ensuring that:

- This policy and procedure is communicated and implemented where applicable.
- Each platform and shared services compiles and implement a site specific procedure encompassing the requirements of this policy and local requirements.
- Resources and facilities are available to implement the requirements of this policy and process.

4. REFERENCES

- Data Retention Policy (COY-IMS-LGL-POL-005)
- Breach Policy (COY-IMS-LGL-POL-006)

5. DEFINITIONS

- "***the Act*"** means the Protection of *Personal Information* Act 4 of 2013;
- "***Data Subject***" means the person to whom *Personal Information* relates, including Company employees;
- "***Deputy Information Officer****"* means any person(s) who have been designated by the Information Officer to perform certain delegated duties and responsibilities of the Information Officer;
- "***Information Officer***" means the head of a private body being either the Chief Executive Officer, the acting Chief Executive Officer or an equivalent officer or any person duly authorized by that officer;
- "***Operator***" means a person who processes *Personal Information* for a *Responsible Party* in terms of a contract of mandate, without coming under the direct authority of that party;

- "***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:
  - 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;
  - information relating to the education or the medical, financial, criminal or employment history of the person;
  - any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
  - the biometric information of the person;
  - the personal opinions, views or preferences of the person;
  - 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;
  - the views of opinions of another individual about the person;
  - 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.
- "***Processing***" means any operation or activity or any set of operations, whether or not by automatic means, concerning *Personal Information*, including:
  - the collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation or use;
  - dissemination 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.
- "***Process***" and "***Processed***" will have the same meaning;
- "***Regulator***" means the Information Regulator established in terms of section 39 of *the Act*;
- "***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*;
- "***Special Personal Information***" means the *Personal Information* referred to in section 26 of the Act, namely Personal Information concerning religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a *Data Subject* or the criminal behaviour of a *Data Subject* to the extent that such information relates to the alleged commission of any offence by the *Data Subject* or any proceedings in respect of any offence allegedly committed by a *Data Subject* or the disposal of such proceedings.

6. POLICY PRINCIPLES

6.1 Lawful Processing of Personal Information

- The Company is required, in the normal exercise of its functions and obligations as a business entity, to process the *Personal Information* of *Data Subjects* from time to time.
- In order to process such *Personal Information,* the Company as a *Responsible Party*, is required to comply with the eight conditions for lawful processing of *Personal Information*, as contained in *the Act*, namely: -
  - Accountability;
  - Processing Limitation;
  - Purpose Specification;
  - Further Processing Limitation;
  - Information Quality;
  - Openness;
  - Security Safeguards; and
  - *Data Subject* Participation.
- The Employees must ensure that they understand and are familiar with the conditions set out above as well as the other provisions of *the Act* in order to ensure lawful processing of *Personal Information* at all times.
- In the event that the Employees are unsure of any issues related to *the Act* or the handling, collection or Processing of *Personal Information*, they must contact the Company's Deputy Information Officer and/or any other person designated by the Company to obtain clarification.

6.2 Conditions for Lawful Processing

- Accountability
  - at the time that the purpose for which the *Personal Information* is being Processed is determined;
  - at the time that the method of Processing such *Personal Information* is determined; and
  - during the Processing of the *Personal Information*.
- Processing Limitation
  - The Processing of the *Personal Information* must be lawful and conducted in a reasonable manner that does not infringe the privacy of the *Data Subject*. The *Personal Information* Processed must, in light of the purpose for the Processing of the *Personal Information*, be adequate, relevant and not excessive.
  - The Company will seek to obtain the consent of all *Data Subjects* prior to the Processing of their *Personal Information*. This informed consent requires that the *Data Subject* should understand the purpose of Processing of the *Personal Information*. Such consent must be obtained in writing.
  - In obtaining consent from a *Data Subject*, the *Data Subject* must be aware that the Company will be responsible for proving that the *Data Subject*'s consent was obtained. Notwithstanding this, failure to obtain such consent will not preclude the Company from Processing the *Personal Information* of *Data Subject*s in certain circumstances where it is permitted in accordance with the provisions of *the Act*.

- Any consent provided by a *Data Subject* may be withdrawn by that *Data Subject* at any time after such consent was obtained by the Company.
- A *Data Subject* may object to the Processing of *Personal Information* at any time, should such information not be utilized for the purposes it was intended for, and should such withdrawal of consent not be in contravention of any legislative requirements and shall not interfere with the ability of the Company to continue to manage the employment relationship.
- A request to withdraw or object to the Processing of the *Personal Information* must be brought to the attention of a responsible person at the Company in writing and in accordance with Annexure A, in order to ensure that the matter is handled appropriately. Any such request for withdrawal of consent must also fully disclose the reason for the request to withdraw consent. In circumstances where the consent is withdrawn, the Company may no longer process the *Personal Information*, unless otherwise permitted in terms of the provisions of the *Act.*

- Purpose Specification
  - The Company may only Process *Personal Information* for a specific, explicitly defined and lawful purpose related to the exercise of its functions and obligations as a business entity. Such purpose must be identified and explained to the Data Subject and must be recorded in the applicable consent forms (where applicable).
  - Subject to the provisions of *the Act*, records of *Personal Information* must not be retained by the Company any longer than is necessary for achieving the purpose for which the *Personal Information* was processed.
  - The Processing of *Personal Information* must be restricted in certain instances as set out in *the Act.* Where the Processing of *Personal Information* is restricted, the Company must inform the *Data Subjects* before lifting the restriction on Processing. The Company will restrict processing of *Personal Information* where: -
    - the accuracy of the *Personal Information* is contested by the *Data Subject* for a period enabling the Company to verify the accuracy of the *Personal Information;*
    - the Company no longer needs the *Personal Information* for achieving the purpose for which the *Personal Information* was collected (but it has to be maintained for purposes of proof);
    - the Processing is unlawful and the *Data Subject* opposes the destruction or deletion of the Personal Information and requests the restriction of its use or the return of the information instead; or
    - the *Data Subject* requests to transmit the *Personal Information* into another automated Processing System.
  - *Personal Information* must be destroyed, deleted or de-identified, in a manner that prevents its reconstruction in an intelligible form, as soon as reasonably practicable once the purpose of its use is met or as soon as the Company is no longer authorised to retain the *Personal Information*, subject to the provisions of *the Act*.

- Further processing limitation
  - The Company may from time to time be required to perform further Processing of *Personal Information*.

- In instances where further Processing of *Personal Information* is required after the initial Processing of the *Personal Information* and the further Processing of *Personal Information* is not compatible with the initial purpose of the Processing of the *Personal Information*, as identified and explained to the *Data Subject*, the Company shall seek to obtain the consent of the *Data Subject* for purposes of such further Processing.
- Notwithstanding this, failure to obtain such consent will not preclude the Company from further Processing of the *Personal Information* of *Data Subject*s in certain circumstances where it is permitted to do so as set out in *the Act*.

- Information Quality

  - The Company's Employees must take reasonably practicable steps to ensure that all Personal Information is complete, accurate, not misleading and updated where necessary, having regard to the purpose for which the Personal Information of Data Subjects is being collected or further processed.

- Openness
  - Having regard to the specific circumstances in which the *Personal Information* is or is not to be Processed, and in accordance with *the Act*, the Company must ensure that the *Data Subjects* are aware of the following before the *Personal Information* is collected or, if collected from any source other than directly from the *Data Subject*s, as soon as reasonably practicable after it has been collected: -
    - *the information being collected and where the Personal Information is not collected from the Data Subject, the source from which it is collected;*
    - *the name and address of the Company, as the Responsible Party;*
    - *the purpose for which the Personal Information is being collected;*
    - *whether or not the supply of the Personal Information by that Data Subject is voluntary or mandatory;*
    - *the consequences of failure to provide the Personal Information;*
    - *any particular law authorising or requiring the collection of the Personal Information;*
    - *the fact that, where applicable, the Company intends to transfer the information to a third country or international organisation and the level of protection afforded to the Personal Information by that third country or international organisation;*
    - *Any further information such as the: -*
      - recipient or category of recipients of the Personal Information;
      - nature or category of the Personal Information;
      - existence of the right of access to and the right to rectify the Personal Information collected;
      - the existence of the right to object to the Processing of Personal Information; and
      - the right to lodge a complaint to the Regulator and the contact details of

the Regulator.

- *The Company has prepared a consent form in terms of which it sets out the above information. Notwithstanding the consent form, it is the responsibility of the Company to ensure that the information is communicated to the Data Subject (where seeking their Personal Information) in accordance with the Act.*

- Security Safeguards
  - The Employees must treat any and all *Personal Information* collected and/or Processed by it as confidential and must not disclose it to any other party and must make every effort to secure the integrity and confidentiality of the *Personal Information* collected by following appropriate procedures regarding security of *Personal Information.*
  - Appropriate, reasonable technical and organisational measures must be taken to prevent loss of, damage to or unauthorised destruction of *Personal Information* and unlawful access to or Processing of *Personal Information*. Any internal or external risks to the *Personal Information* must be reported by the Employees to one of the Company's Deputy or Information Officers or any other person designated by the Company.
  - The Company may appoint Operators to Process *Personal Information* and to establish and maintain security measures to safeguard against any risks identified. Such Operator will only process such information with the knowledge and authorisation of the Company and must treat the *Personal Information* as confidential and not disclose it. Such Operator will notify the Company where there are reasonable grounds to believe that the *Personal Information* of *Data Subjects* has been accessed or acquired by an unauthorised person.
  - Should the confidentiality of the *Personal Information* be compromised, this must be reported as soon as reasonably possible to the Company's Deputy or Information Officer and/or any other designated person at the Company. The Regulator must be notified and the *Data Subject* must be notified in writing informing the *Data Subject* of any protective measures the Company intends to take.

- *Data Subject* Participation
  - The *Data Subject* may, after providing adequate proof of their identity, request access to relevant *Personal Information*, which must then be provided to the *Data Subject*.
  - The Company may refuse access where the provisions of the Promotion of Access to Information Act are applicable.
  - The *Data Subject* must be advised of the right to correct the *Personal Information*.
  - The *Data Subject* may request that their *Personal Information* be corrected or deleted or that a record containing *Personal Information* of the *Data Subject* be destroyed or deleted if the *Data Subject* believes that the *Personal Information* or record of the *Personal Information* is: -
    - *inaccurate;*
    - *irrelevant;*
    - *excessive;*
    - *out of date;*

- *incomplete;*
- *misleading; or*
- *has been obtained unlawfully.*

– If the Company receives such a request it must, as soon as reasonably practicable, and in compliance with *the Act*: -

- *correct the Personal Information;*
- *destroy or delete the Personal Information;*
- *provide the Data Subject, to his or her satisfaction, with credible evidence in support of the Personal Information; or*

– where agreement cannot be reached between the Company and the *Data Subject*, and if the *Data Subject* so requests, take such steps as are reasonable in the circumstances to attach to the information in such a manner that it will always be read with the information, an indication that a correction of the information has been requested but has not been made.

6.3 Processing of Special *Personal Information*

The Company will seek to obtain the specific consent of all *Data Subject*s to the Processing of their Special *Personal Information*. Notwithstanding this, failure to obtain such consent will not preclude the Company from Processing the Special *Personal Information* in certain circumstances where it is expressly permitted to do so in accordance with the provisions of *the Act*.

6.4 Personal Information of Employees and Job Applicants

In addition to what has been set out above, the following principles are particularly important in respect of the *Personal Information* of the Employees and job applicants.

7. RECRUITMENT AND APPOINTMENT

– The Company may, from time to time, need to Process various *Personal Information* about a job applicant in connection with the recruitment process. The Company will ensure that when processing a job applicant's *Personal Information*, it will adhere to its obligations in accordance with the provisions of *the Act*.
– In addition, and as a consequence of the employment relationship entered into between the Company and its employees, the Company will Process various *Personal Information* about an Employee in connection with the employment relationship. The Company will ensure that in processing an Employee's *Personal Information*, it will adhere to its obligations in accordance with the provisions of *the Act*.
– The Company will take reasonably practicable steps to ensure that the job applicant or the Employee understands the purpose for the Processing of their *Personal Information* and that informed consent is obtained from the Job Applicant or the Employee prior to processing any of their *Personal Information*.
– Notwithstanding this, failure to obtain such consent will not preclude the Company from Processing the *Personal Information* in certain circumstances where it is permitted to do so in accordance with the provisions of *the Act*.

- The Company must collect *Personal Information* from the job applicant or the employee directly unless the information is derived from a public record or has been deliberately made public by the job applicant or the employee.
- The Company will take all reasonable steps to ensure that the job applicant's *Personal Information* will only be used for purposes connected to recruitment and marketing purposes related to recruitment and the employment relationship.

8. STORAGE OF *PERSONAL INFORMATION* OF EMPLOYEES

- The Company will seek to obtain the consent of all Data Subjects to the transfer of their Personal Information between South Africa and other international countries.
- In obtaining such consent from a *Data Subject*s and/or Employees, *Data Subject*s must be aware that the Company will be responsible for proving that the *Data Subject*s and/or the Company's Employee's consent was obtained. Notwithstanding this, failure to obtain such consent will not preclude the Company from transferring the *Personal Information* of *Data Subject*s in certain circumstances where it is permitted to do strictly as set out in *the Act*.
- The remainder of the *Personal Information* is contained in personnel files which are safely kept in the Human Resources Department, to which access is limited.
- Upon termination of employment with the Company, *Personal Information* will be handed to the relevant Operators for the purposes of post-employment benefits, if any, and save as required by law, thereafter will be destroyed, deleted and/or de-identified.

9. RETENTION OF *PERSONAL INFORMATION* AFTER TERMINATION OF EMPLOYMENT

The Company shall destroy all hard copies of a terminated employee's *Personal Information* in accordance with the Company's Data Retention Policy.

10. DISTRIBUTION OF *PERSONAL INFORMATION* TO THIRD PARTIES

- The Company may provide access to or transfer an Employee's *Personal Information* where it is necessary for the purposes for which the *Personal Information* is processed. Such third parties include but are not limited to the Company's branches, subsidiaries or affiliated companies, the Company's registered clients, parties providing products and services to the Company, regulatory authorities or as required by law.
- Third parties are to adhere to the provisions of POPI Act and establish and maintain the necessary safeguards in accordance with the provisions of *the Act*.
- They must also familiarise themselves with the Client's POPI policies and procedures and ensure its compliance with the provisions thereof, as amended from time to time.

11. TRANSBORDER INFORMATION FLOWS

- The Company will only transfer the *Personal Information* of a data subject to a third party who is in a foreign country if: -
  - *The third party is subject to a law, binding corporate rules or binding agreement which provides an adequate level of protection and which are substantially similar to the conditions of lawful processing in POPI and which includes provisions which*

are substantially similar to section 72 of POPI; or

- *The Data Subject consents to the transfer; or*
- *The transfer is necessary for the performance of a contract between the Data Subject and the Company; or*
- *The transfer is necessary for the implementation of pre-contractual measures taken in response to the Data Subject's request; or*
- *The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Company and a third party; or*
- *The transfer is for the benefit of the Data Subject and it is not reasonably practicable to obtain his/her/its consent and if such consent could have been obtained the data subject would have given it.*

12. INFORMATION OFFICER

- The Group Chief Executive Officer of the Company duly authorized the Group Human Resources Executive of the Company to be designated as the Company's Information Officer and he shall perform the duties set out in *the Act* and be responsible for all issues dealt with in this policy.
- The Company shall also appoint one Deputy Information Officer as it deems necessary to assist the Information Officer and to comply with section 56 of *the Act*.

13. REVIEW

Changes to the Act and its Regulations will be monitored by the Company and further amendments may be required to this policy in order for the Company to remain compliant with its legal obligations.

---End of document---