




# POPIA POLICY

**TABLE OF CONTENTS**

<b>1. Introduction</b>	<b>3</b>
<b>2. Important Notice</b>	<b>3</b>
<b>3. Definitions, Acronyms and Abbreviations</b>	<b>3</b>
<b>4. Purpose</b>	<b>4</b>
<b>5. Application of this Policy</b>	<b>4</b>
<b>6. Rights of Data Subjects</b>	<b>4</b>
<b>7. General Guiding Principles</b>	<b>6</b>
7.1. Accountability	6
7.2. Processing Limitation	6
7.3. Purpose Specification	6
7.4. Further Processing Limitation	7
7.5. Information Quality	8
7.6. Openness	8
7.7. Security Safeguards	8
7.8. Data Subject Participation	8
<b>8. Processing of Special Personal Information</b>	<b>9</b>
<b>9. Compliance with the Policy</b>	<b>9</b>
<b>10. Personnel and Authorized Third Parties</b>	<b>10</b>
<b>11. Request to Access Personal Information Procedure</b>	<b>11</b>
<b>12. Cross-Border Transfer of Personal Information / Data Storage and Retention</b>	<b>11</b>
<b>13. Processing of Personal Information of Personnel</b>	<b>12</b>
<b>14. Complaints Procedure</b>	<b>13</b>
<b>15. Enforcement and Reporting of Breaches of this Policy</b>	<b>13</b>
<b>16. Effective Date and Policy Review</b>	<b>14</b>

	<b>Legaro Property Development</b>	Page 3 of 14
	Legal	
	<b>POPIA POLICY</b>	

**1. Introduction**

- 1.1 Through the conduct of its business activities, Legaro Property Development registration number: 2017/084528/07 (the “Legaro” / “we” / “us” / “our”) processes (including collects, uses, stores, disseminates and disposes of) personal information of clients, suppliers, employees and/or other stakeholders (collectively, data subjects as defined below).
- 1.2 Legaro is committed to effectively and efficiently managing personal information in accordance with the Protection of Personal Information Act, 4 of 2013 and any regulations (“POPIA”).
- 1.3 This privacy policy (“Policy”) is intended to govern Legaro’s processing of personal information of clients, suppliers, employees and/or other stakeholders.


**2. Important Notice**

Please read the terms of this Policy carefully to understand our views and practices regarding personal information and how we will treat it.

**3. Definitions, Acronyms and Abbreviations**

Unless otherwise determined by the context the words and expressions used un this Policy shall bear the meaning assigned to them below –


- 3.1 "child" a natural living person under the age of 18.
- 3.2 "consent" means any voluntary, specific and informed expression of will in terms of which permission is given for processing of personal information.
- 3.3 "Data subject" a person to whom personal information relates.
- 3.4 "de-identify" means to delete any personal information that identifies a data subject, or which can be used by a reasonably foreseeable method to identify or when linked to other information that identifies the data subject and the term “de-identifies” shall have a corresponding meaning;
- 3.5 "direct marketing" means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of: (i) promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or (ii) requesting the data subject to make a donation of any kind for any reason;
- 3.6 "Deputy information officer" means the Head of Legal of Legaro, whose responsibility is to ensure the organization’s compliance with PoPIA;
- 3.7 "Information regulator" means the information regulator established in terms of section 39 of PoPIA;
- 3.8 "Legitimate basis" means any of the following legitimate bases recognized by PoPIA for the processing of personal information –
  - 3.8.1 the data subject, or a competent person where the data subject is a child, consents to the processing; or
  - 3.8.2 the processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; or
  - 3.8.3 the processing complies with an obligation imposed by law on the responsible party; or
  - 3.8.4 the processing protects a legitimate interest of the data subject; or
  - 3.8.5 the processing is necessary for pursuing the legitimate interests of Legaro or of a third party to whom the information is supplied.

	<b>Legaro Property Development</b>	Page 4 of 14
	Legal	
	<b>POPIA POLICY</b>	

- 3.9 "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 the responsible party;
- 3.10 "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 –
- 3.10.1 information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, color, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
  - 3.10.2 information relating to the education or the medical, financial, criminal or employment history of the person;
  - 3.10.3 any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
  - 3.10.4 the biometric information of the person;
  - 3.10.5 the personal opinions, views or preferences of the person;
  - 3.10.6 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;
  - 3.10.7 the views or opinions of another individual about the person; and
  - 3.10.8 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;
- 3.11 "processing / process" means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including –
- 3.11.1 the collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation or use;
  - 3.11.2 dissemination by means of transmission, distribution or making available in any other form; or
  - 3.11.3 merging, linking, as well as restriction, degradation, erasure or destruction of information;
- 3.12 "re-identify" means, in relation to personal information of a data subject, to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject;
- 3.13 "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 of personal information; and
- 3.14 "special personal information" means personal information relating to: (i) the 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 (ii) the criminal behavior of a data subject to the extent that such intimation relates to: (a) the alleged commission by a data subject of any offence; or (b) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

#### 4. **Purpose**

- 4.1 The purpose of this Policy is to protect Legaro from the compliance risks associated with the protection of personal information under PoPIA and to ensure that Legaro processes personal information in a manner that demonstrates its commitment to the privacy of data subjects.
- 4.2 This Policy demonstrates Legaro's commitment to protecting the privacy rights of data subjects in the following manner –

	<b>Legaro Property Development</b>	Page 5 of 14
	Legal	
	<b>POPIA POLICY</b>	

- 4.2.1 through stating desired behavior and directing compliance with the provisions of PoPIA and best practices;
- 4.2.2 by developing and implementing internal controls for the purpose of managing the compliance risk associated with the processing of personal information;
- 4.2.3 by creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate interests of Legaro; and
- 4.2.4 by assigning specific duties and responsibilities to control owners, including the appointment of an deputy information officer to ensure compliance with PoPIA and where necessary, in order to protect the interests of Legaro and data subjects.

## 5. **Application of this Policy**

### 5.1 This Policy applies to –

- 5.1.1 all employees, directors, officers and other staff of Legaro ("**Personnel**"); and
- 5.1.2 all third parties who process the personal information of Legaro's data subjects on behalf of Legaro or as part of any functions or duties which they carry out (whether contractual or otherwise) for Legaro ("**Authorized Third Parties**").

5.2 The legal duty to comply with PoPIA's provisions and this Policy is activated in any situation where there is: processing of personal information by or for a responsible party domiciled within the Republic of South Africa or a responsible party not domiciled in the Republic of South Africa but making use of automated or non-automated means in the Republic of South Africa to process personal information.

5.3 This Policy is applicable to the processing of all personal information throughout the information life cycle, from the point of first collection of personal information until the time that such information is destroyed.

5.4 This Policy should be read in conjunction with all other relevant policies of Legaro regulating privacy and protection of information.

5.5 This Policy will not apply in situations where the processing of personal information –

- 5.5.1 is concluded in the course of purely personal or household activities; or
- 5.5.2 where the personal information has been de-identified.

## 6. **Rights of Data Subjects**

6.1 Legaro must ensure that its data subjects (including clients, suppliers and other persons in respect of whom personal information is processed) are made aware of the rights conferred upon them as data subjects.

6.2 In carrying out its processing activities, where Legaro is a responsible party, Legaro must ensure that it gives effect to the following rights enshrined under PoPIA –

### 6.2.1 The rights to access personal information

Legaro recognizes that a data subject has the right to establish whether Legaro holds personal information related to him, her or it, including the right to request access to that personal information, where such personal information is held by Legaro.

### 6.2.2 The right to have personal information corrected or deleted

Legaro recognizes that a data subject has the right to request, where necessary, that his, her or its personal information must be corrected or deleted where Legaro is no longer authorized to retain the personal information.



- 6.2.3 The right to object to the processing of personal information  
Legaro recognizes that a data subject has the right, on reasonable grounds, to object to the processing of his, her or its personal information. In such circumstances, Legaro will give due consideration to the request and the requirements of PoPIA.
- 6.2.4 The right to object to direct marketing  
Legaro recognizes that a data subject has the right to object to the processing of his, her or its personal information for purposes of direct marketing.
- 6.2.5 The right to complain to the information regulator  
Legaro recognizes that a data subject has the right to submit a complaint to the information regulator regarding an alleged infringement of any of the rights protected under PoPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its personal information.
- 6.2.6 The right to be informed  
Legaro recognizes that a data subject has the right to be notified that his, her or its personal information is being collected by Legaro. The data subject also has the right to be notified in any situation where the organization has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorized person.

7. **General Guiding Principles**

All Personnel and/or Authorized Third Parties must always be subject to, and act in accordance with, the following guiding principles –


7.1 **Accountability**

- 7.1.1 Legaro will ensure that the provisions of PoPIA and the guiding principles outlined in this Policy are complied with through the encouragement of desired behavior. However, Legaro will take appropriate sanctions, which may include disciplinary action, against those individuals who through their intentional or negligent actions and/or omissions fail to comply with the principles and responsibilities outlined in this Policy.
- 7.1.2 Failing to comply with PoPIA could potentially damage Legaro's reputation, expose Legaro to administrative fines or expose Legaro to civil claims for damages. The protection of personal information is therefore the responsibility of all Personnel and Authorized Third Parties.

7.2 **Processing Limitation**

- 7.2.1 Legaro must ensure that personal information under its control is processed: (i) in a fair, lawful and non-excessive manner; (ii) only where a legitimate basis exists; and (iii) only for a specifically defined purpose.
- 7.2.2 Legaro must inform the data subject(s) of the reasons for collecting his, her or its personal information and ensure that there is a legitimate basis prior to processing personal information. This may include having to obtain the consent of the data subject prior to processing personal information. If any Personnel or Authorized Third Parties' are unsure about whether there is a justifiable legal basis for processing personal information, please contact the deputy information officer.
- 7.2.3 Where applicable, the data subject must be informed of the possibility that their personal information will be shared with third parties and/or affiliates of Legaro and be provided with the reasons for doing so.

7.3 **Purpose Specification**

	<b>Legaro Property Development</b>	Page 7 of 14
	Legal	
	<b>POPIA POLICY</b>	

- 7.3.1 All of Legaro's business units' and/or operations' processing must be informed by the principle of transparency.
- 7.3.2 Legaro must process personal information only for specific, explicitly defined and legitimate reasons. Where it is practical to do so, Legaro must inform data subjects of these reasons prior to collecting or recording the data subject's personal information.

**7.4 Further Processing Limitation**

- 7.4.1 Personal information must not be processed for a secondary purpose, unless that secondary purpose is compatible with the original purpose.
- 7.4.2 In this regard, PoPIA provides that further processing is not incompatible with the purpose of collection if: (i) the data subject (or a competent person the case of a child's personal information) has consented to the further processing; (ii) the information has been deliberately made public by the data subject or is available in or derived from a public record; (iii) further processing is necessary to avoid prejudice to maintenance of the law by any public body; for compliance with an obligation under law generally or to enforce legislation concerning the collection of revenue; for conduct of judicial proceedings; in the interests of national security; to prevent a serious and imminent threat to public health or safety or the life or health of the data subject or any other individual; or the personal information is used solely for historical, statistical or research purposes and the responsible party ensures that the personal information will not be published in an identifiable form; or the further processing falls in accordance with an exemption granted by the information regulator in terms of PoPIA. Therefore, where Legaro seeks to process personal information, it holds for a purpose other than the original purpose for which it was originally collected, and where this secondary purpose is not compatible with the original purpose, Legaro must first obtain additional consent from the data subject.

**7.5 Information Quality**


- 7.5.1 Legaro must take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading.
- 7.5.2 Where personal information is collected or received from third parties, Legaro must take reasonable steps to confirm that the information is correct by verifying the accuracy of the information directly with the data subject or by way of independent sources.

**7.6 Openness**

Legaro must take reasonably practicable steps to ensure that the data subject is aware of the processing. PoPIA requires Legaro to disclose to the data subject certain information including the following: (i) what information is being processed; (ii) who has access to such information (e.g. whether the information will be transferred to any third parties, including third parties outside of the Republic of South Africa); and (iii) what the consequences will be should the data subject refuse to provide such information.

**7.7 Security Safeguards**

- 7.7.1 Legaro must take all reasonable precautions, with regard to the nature of the personal information and the risks of the processing, to preserve the security of the personal information and, in particular, prevent its alteration, loss and damage, or access by non-authorized persons. PoPIA requires Legaro to ensure the security and integrity of personal information in its possession or under its control with appropriate, reasonable technical and organizational measures to prevent loss, unlawful access and unauthorized destruction of personal information.

	<b>Legaro Property Development</b>	Page 8 of 14
	Legal	
	<b>POPIA POLICY</b>	

- 7.7.2 Legaro must put in place measures (having regard to generally accepted information security practices or industry specific requirements or professional rules) to identify internal and external security risks; maintain safeguards against such risks; regularly verify that the safeguards are effective and continually update safeguards in response to new risks.
- 7.7.3 Legaro must ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorized individuals.
- 7.7.4 All new Personnel will be required to sign contracts containing contractual terms for the use and storage of information. Confidentiality clauses should be included in all contracts with operators to reduce the risk of unauthorized disclosures of personal information for which Legaro is responsible.

**7.8 Data Subject Participation**

In terms of PoPIA, a data subject is entitled to request that its personal information is corrected, updated and deleted and Legaro is required to take reasonably practicable steps to ensure that personal information is complete, accurate, not misleading and is updated from time to time to the extent that Legaro is in possession of such information. In light of this, Legaro must facilitate access to all personal information processed on request by a data subject by way of the PAIA Manual.

**8. Processing of Special Personal Information**

- 8.1 Subject to exceptions, PoPIA provides that all processing of special personal information is generally prohibited.
- 8.2 The main exemptions to the general prohibition are: (i) where the data subject has given his/her/its express consent; or (ii) processing is necessary for the establishment, exercise or defense of a right or obligation in law; (iii) information has deliberately been made public by the data subject; (iv) the processing of special personal information is for historical, statistical or research purposes to the extent that such purposes are: (a) in the public interests; or (b) it would have been impossible to ask for consent, and appropriate safeguards have been put in place to protect the personal information of the data subject.
- 8.3 In the event that Legaro's processing of personal information concerns special personal information, such processing must be carried out in line with the relevant provisions of PoPIA.
- 8.4 If you are unsure about whether any personal information constitutes special personal information and/or whether there is a legal basis for processing such special personal information, please contact the deputy information officer.
- 8.5 Legaro must only disclose special personal information to another person when –
  - 8.5.1 the consent of the data subject has been obtained for such disclosure;
  - 8.5.2 directed by an order of a court; and/or
  - 8.5.3 required in terms of any applicable law.
- 8.6 Legaro may not process any personal information concerning a child and will only do so where it has obtained the consent of the parent or guardian of that child or where Legaro is permitted to do so in accordance with applicable laws.

**9. Compliance with the Policy**

- 9.1 The deputy information officer is responsible for ensuring that this Policy is implemented throughout Legaro.
- 9.2 The deputy information officer is responsible for, *inter alia* –
  - 9.2.1 taking steps to ensure Legaro's reasonable compliance with the provision of PoPIA;




- 9.2.2 keeping Legaro updated about Legaro's personal information protection responsibilities under PoPIA. For instance, in the case of a security breach, the deputy information officer must inform and advise Legaro of their obligations under PoPIA;
- 9.2.3 continually assessing Legaro's personal information processing procedures and aligning them with applicable laws, privacy regulations and best practices. This will include reviewing Legaro's information protection procedures and related policies;
- 9.2.4 ensuring that Legaro makes it convenient for data subjects who want to update their personal information or submit PoPIA related complaints to Legaro;
- 9.2.5 approving any contracts entered into with Personnel and Authorized Third Parties. This will include overseeing the amendment of Legaro's employment contracts and other data processing agreements, where applicable;
- 9.2.6 encouraging compliance with the conditions required for the lawful processing of personal information;
- 9.2.7 ensuring that Personnel and other persons acting on behalf of the organization are fully aware of the risks associated with the processing of personal information and that they remain informed about the organization's security controls;
- 9.2.8 organizing and overseeing the awareness training of Personnel and other individuals involved in the processing of personal information on behalf of Legaro;
- 9.2.9 addressing Personnel's and Authorized Third Party's PoPIA related questions;
- 9.2.10 addressing all PoPIA related requests and complaints made by Legaro's data subjects; and
- 9.2.11 working with the information regulator in relation to any ongoing investigations.

**10. Personnel and Authorized Third Parties**

- 10.1 Personnel and/or Authorized Third Parties will, during the course of the performance of their duties and/or services, gain access to and become acquainted with the personal information of certain employees, clients and suppliers of Legaro.
- 10.2 Personnel and/or Authorized Third Parties are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.
- 10.3 Personnel and/or Authorized Third Parties may not directly or indirectly, utilize, disclose or make public in any manner to any person or third party, either within Legaro or externally, any personal information, unless such information is already publicly known or the disclosure is necessary in order for the relevant Personnel and/or Authorized Third Parties to perform his, her or its duties.
- 10.4 Personnel and/or Authorized Third Parties must request assistance from their line manager or the deputy information officer if they are unsure about any aspect related to the protection of a data subject's personal information.
- 10.5 Personnel and/or Authorized Third Parties must only process personal information where a legitimate basis exists for such processing.
- 10.6 Furthermore, personal information must only be processed where the data subject clearly understands why and for what purpose his, her or its personal information is being collected and processed.
- 10.7 Where the legal basis for processing is consent, Personnel and/or Authorized Third Parties will, prior to processing any personal information, obtain the data subject's consent.
- 10.8 Consent to process a data subject's personal information must be obtained directly from the data subject, except where exceptions apply, such as (*inter alia*) –
  - 10.8.1 the personal information has been made public;



- 10.8.2 where valid consent has been given to a third party; or
- 10.8.3 the information is necessary for effective law enforcement.
- 10.9 Personnel and/or Authorized Third Parties will under no circumstances –
  - 10.9.1 process or have access to personal information where such processing or access is not a requirement to perform their respective work-related tasks or duties;
  - 10.9.2 save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smart phones;
  - 10.9.3 share personal information through unsecure methods. Where access to personal information is required, this may be requested from the relevant line manager or the deputy information officer; and
  - 10.9.4 transfer personal information outside of the Republic of South Africa without the express permission from the deputy information officer.
- 10.10 Personnel and/or Authorized Third Parties are responsible for –
  - 10.10.1 keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this Policy and any other applicable policies related to information security or record keeping;
  - 10.10.2 ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created;
  - 10.10.3 where possible, ensuring that personal information is encrypted prior to sending or sharing the information electronically;
  - 10.10.4 ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorized persons;
  - 10.10.5 ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks. Ensuring that where personal information is stored on removable storage medias such as external drives, flash sticks, CDs or DVDs that these are kept locked away securely when not being used;
  - 10.10.6 ensuring that where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorized people cannot access it. For instance, in a locked drawer of a filing cabinet;
  - 10.10.7 ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorized individuals could see or copy them. For instance, close to the printer;
  - 10.10.8 taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the client phones or communicates via email. Where a data subject's information is found to be out of date, authorization must first be obtained from the relevant line manager or the deputy information officer to update the information accordingly;
  - 10.10.9 taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorization must first be obtained from the deputy information officer to delete or dispose of the personal information in the appropriate manner;

	<b>Legaro Property Development</b>	Page 11 of 14
	Legal	
	<b>POPIA POLICY</b>	

10.10.10 from time to time, undergoing PoPIA awareness training, as may be required by Legaro; and

10.10.11 where Personnel and/or Authorized Third Parties becomes aware or suspicious of any security breach such as the unauthorized access, interference, modification, destruction or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to the deputy information officer.

10.11 Where necessary or appropriate, agreements with Authorized Third Parties to whom Legaro may disclose personal information must be concluded to ensure that they process any personal information in accordance with the provisions of this Policy and PoPIA. All such Authorized Third Parties should at the very least conclude non-disclosure agreements with Legaro compelling them to secure and treat all personal information in their possession as confidential and preventing such third parties from disclosing such information.

10.12 All Authorized Third Parties who process personal information must strictly adhere to the security requirements set forth in this Policy and to Legaro's security policy(ies) and shall be required to maintain and where required, upgrade their systems and processes to comply with the terms of this Policy and such security policies.

10.13 Legaro must carry out a due diligence of all Authorized Third Parties processing personal information on behalf of Legaro and this may include auditing the facilities, security procedures and policies of such Authorized Third Parties.

10.14 Authorized Third Parties must immediately inform Legaro (*via* the office of the deputy information officer) of any actual or suspected security breach or compromise to personal information in its possession. The Authorized Third Parties may be required to notify the affected data subject(s) and the information regulator, but this should only be carried out on Legaro's instructions, *via* the office of the deputy information officer.

## **11. Request to Access Personal Information Procedure**

11.1 Data subjects have the right to –

11.1.1 request information about personal information Legaro holds about them and request reasons for holding it;

11.1.2 request access to their personal information. Access to such personal information can be requested by email, addressed to the deputy information officer. The deputy information officer will process all requests within a reasonable time; and

11.1.3 be informed how to keep their personal information up to date.

11.2 All requests for access received by Legaro should be addressed by the office of the deputy information officer only and should any Legaro staff member receive such a request, it should be immediately furnished to the office of the deputy information officer and can be emailed to the following address: [info@legaro.co.za](mailto:info@legaro.co.za)

## **12. Cross-Border Transfer of Personal Information**

12.1 PoPIA provides that a responsible party may not transfer personal information about a data subject to a third party in a foreign jurisdiction unless –


12.1.1.1 the recipient's country is subject to a law or the recipient is bound by a contract which upholds principles of reasonable processing of the information that are substantially similar to the principles contained in PoPIA; and



- 12.1.1.2 includes provisions that are substantially similar to those contained in PoPIA relating to the further transfer of personal information from the recipient to third parties; or
- 12.1.2 the data subject consents to the transfer; or
- 12.1.3 the transfer is necessary for the performance of a contract between the data subject and responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request; or
- 12.1.4 the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party; or
- 12.1.5 the transfer is for the benefit of the data subject, and –
  - 12.1.5.1 it is not reasonably practicable to obtain the consent of the data subject to that transfer; and
  - 12.1.5.2 if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.
- 12.2 In carrying out any cross-border transfers, Legaro must adhere to the provisions of PoPIA. For instance, Legaro can send or transfer personal information of data subjects to Legaro's group companies (where applicable) and/or Authorized Third Parties beyond the borders of the Republic of South Africa in order to achieve the purpose for which the personal information was collected and processed, including for processing and storage by Authorized Third Parties, if the applicable data subject(s) has consented to such cross-border transfer.
- 12.3 Any cross-border transfers of personal information should be brought to the attention of, and authorised by, the deputy information officer

**13. Data Storage and Retention**

- 13.1 Legaro and/or Authorized Third Parties must ensure that personal information, including special personal information and any commercially sensitive information which it processes is captured, used, disclosed, stored and destroyed in a secure and confidential manner appropriate to the classification of the information, in accordance with Legaro's IT Policy and / or relevant provisions of PoPIA and other applicable laws.
- 13.2 Authorized Third Parties, including data storage and processing providers, may from time to time also have access to a data subject's personal information in connection with the storage and retention thereof. Legaro must ensure that these Authorized Third Parties only process the personal information in accordance with the provisions of this Policy, all other relevant internal policies of Legaro and PoPIA.
- 13.3 In order to comply with PoPIA, Legaro—
  - 13.3.1 must keep records of the personal information it has collected, correspondence or comments in an electronic or hardcopy file format. Personal information may be processed for as long as necessary to fulfil the purposes for which that personal information was collected and/or as permitted or required by applicable law;
  - 13.3.2 may retain personal information for longer periods for statistical, historical or research purposes, and should this occur, Legaro must ensure that appropriate safeguards have been put in place to ensure that all recorded personal information will continue to be processed in accordance with this Policy and the applicable laws; and
  - 13.3.3 must, once the purpose for which the personal information was initially collected and processed no longer applies or becomes obsolete, ensure that it is deleted, destroyed or de-identified so that a third party cannot re-identify such personal information.

	<b>Legaro Property Development</b>	Page 13 of 14
	Legal	
	<b>POPIA POLICY</b>	


#### 14. **Processing of Personal Information of Personnel**

- 14.1 Legaro's human resource function ("HR") shall ensure that they comply with this Policy in respect of all Legaro's Personnel data which they have on file and collect and which falls within the definition of personal information, including that HR will only collect such personal information of Personnel as is necessary for their employment relationship with Legaro. This includes information collected from the time that a potential member of Personnel applies for a job, during the interview and selection process and if such candidate is successful, all information processed during the course of their employment and on the termination of their employment.
- 14.2 The appropriate consent forms should be included as part of the terms of engagement and/or employment contracts concluded with each of the Personnel.

#### 15. **Complaints Procedure**

Data subjects have the right to complain in instances where any of their rights under PoPIA have been infringed upon. Legaro takes all complaints very seriously and will address all PoPIA related complaints in accordance with the following procedure –Complaints in terms of PoPIA must be submitted to Legaro's Information Officer in writing as follows –

- 15.1 by post: Suite 8 Private Bag X16, Craighall, 2047
- 15.1.1 by e-mail: [info@legaro.co.za](mailto:info@legaro.co.za)
- 15.2 Where the complaint has been received by any person other than the deputy information officer, that person will ensure that the full details of the complaint reach the deputy information officer within 3 (three) working days.
- 15.3 The deputy information officer will provide the complainant with a written acknowledgement of receipt of the complaint within 5 (five) working days.
- 15.4 The deputy information officer will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the information officer
- 15.5 The deputy information officer must also determine whether the complaint relates to an error or breach of confidentiality that has occurred and which may have a wider impact on Legaro's data subjects.
- 15.6 Where the deputy information officer has reason to believe that the personal information of data subjects has been unlawfully accessed or acquired by an unauthorised person, the deputy information officer will consult with Legaro's Executive Committee, where after, the affected data subjects and the information regulator will be informed of the breach.
- 15.7 The deputy information officer will revert to the complainant with a proposed solution with the option of escalating the complaint to Legaro's Executive Committee within 20 (twenty) working days of receipt of the complaint. In all instances, Legaro will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.
- 15.8 The deputy information officer's response to the data subject may comprise any of the following
- 15.8.1 a suggested remedy for the complaint;
- 15.8.2 a dismissal of the complaint and the reasons as to why it was dismissed; and/or
- 15.8.3 an apology (if applicable) and any action proposed to be taken.
- 15.9 Where the data subject is not satisfied with the deputy information officer's suggested remedies, the data subject has the right to complain to the information regulator. The website of the information regulator can be accessed at the following link: <http://justice.gov.za/inforeg/>. The information regular can be contacted at the following details:

	<b>Legaro Property Development</b>	Page 14 of 14
	Legal	
	<b>POPIA POLICY</b>	

15.9.1 Tel: (+27)12 406 4818

15.9.2 Fax: (+27)86 500 3351

15.9.3 Email: [infoleg@justice.gov.za](mailto:infoleg@justice.gov.za)

15.10 The deputy information officer will review the complaints process to assess the effectiveness of the procedure on a periodic basis and to improve the procedure where it is found wanting. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to PoPIA related complaints.

#### **16. Enforcement and Reporting of Breaches of this Policy**

16.1 Any non-compliance with the terms of this Policy could have serious legal and reputational repercussions for Legaro and may cause significant damage to Legaro. Therefore, any non-compliance could lead to disciplinary action being taken against the relevant Personnel.

16.2 Should any Personnel become aware of any non-compliance with the terms of this Policy, they are required to immediately report this to their relevant line managers, who in turn should report this to the deputy information officer. Such reports may also be sent to the following email address: [infor@legaro.co.za](mailto:infor@legaro.co.za)

#### **17. Effective Date and Policy Review**

No deviation to this Policy shall be allowed.

This Policy will be reviewed at regular intervals when appropriate, to ensure it deals appropriately with Legaro's processing of personal information. Any change required to this policy should be made in accordance with the Control of Documents Procedure (PRO-IMS-001) and must be approved by the deputy information officer.