

# Privacy of Personal Information Act Policy

## 1 Accountability

- 1.1 Kevin Lourens is hereby appointed as the Personal Information Compliance Officer (the "Officer") for Axiam Capital Management (Pty) Ltd ("Axiam"). Grant Dykes is appointed as the deputy Personal Information Officer.
- 1.2 Data subjects are defined as any clients (persons or entities) investing with Axiam or any suppliers or other parties providing personal information to Axiam.
- 1.3 All Persons (Responsible Party), whether employees, volunteers, board or committee members who collect, process, or use personal information, shall be accountable for such information to the Officer.
- 1.4 This Policy shall be made available via the Axiam website ([www.axiam.co.za](http://www.axiam.co.za)).
- 1.5 This Policy will be made available via electronic copy provided upon written request.
- 1.6 Any personal information transferred to a third party for processing is subject to this Policy. The Officer shall use contractual or other appropriate means to protect personal information at a level comparable to this Policy while a third party is processing this information.
- 1.7 Personal information to be collected, retained, or used by Axiam shall only be done after the Officer has given approval. This information shall be secured according to the Officer's instructions.
- 1.8 Any data subject who believes Axiam uses personal information collected, retained, or used for purposes other than those that the data subject explicitly approved may contact the Officer to register a complaint or make any related inquiry.
- 1.9 Upon receiving a complaint from any person regarding the collection, retention, or use of personal information, the Officer shall promptly investigate the complaint and notify the person who complained about their findings and corrective action taken, if any.
- 1.10 The Officer shall communicate and explain this Policy and give training to all employees and volunteers who might collect, retain, or use personal information.

## **2 Identifying Purposes**

- 2.1 The Officer shall document the purpose for which personal information is collected to comply with the openness and individual access principles outlined below.
- 2.2 The Officer shall determine the information needed to fulfil the purposes for which the information is collected. To comply with the collection principle below:
  - 2.2.1 The Officer shall ensure that the purpose is specified at or before the time of collecting the personal information from an individual/company.
  - 2.2.2 The Officer shall ensure that the information collected will not be used for any other purpose before obtaining the individual's approval, unless the new purpose is required by law.
  - 2.2.3 The Officer shall ensure that a person collecting personal information will be able to explain to the individual why this is being done.
  - 2.2.4 The Officer shall ensure that limited collection, limited use, disclosure, and retention principles are respected in identifying why personal information is collected.

## **3 Consent**

- 3.1 The Officer shall ensure that the individual/company from whom personal information is collected consents to this and to it being used and disclosed.
- 3.2 The Officer shall ensure that the individual/company can reasonably understand why and how the information will be used when the consent is given.
- 3.3 The Officer shall ensure that no condition is attached to supplying benefits because of Axiom's activities, requiring the individual/company to consent to collecting, using, or disclosing information beyond necessary to fulfil the explicitly specified and legitimate purposes.
- 3.4 The Officer shall ensure that express consent is obtained wherever possible and appropriate. In rare circumstances where, in the Officer's opinion, regarding the information's sensitivity and the Policy's purpose and intent, implied consent might be acceptable.
- 3.5 In obtaining consent, the Officer shall ensure that the individual's reasonable expectations are respected.
- 3.6 The Officer shall ensure that the express consent obtained from an individual is explicit and in an appropriately verifiable form.
- 3.7 The Officer shall ensure that the individual/company may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The individual/company shall promptly be informed of the withdrawals implications.

## **4 Limiting Collection**

- 4.1 The Officer shall ensure that personal information will not be collected indiscriminately. The amount and the type of information collected shall be limited to what is necessary to fulfil the purposes identified. The Officer shall specify the type of information to be collected according to the openness principle.
- 4.2 The Officer shall ensure that the information is collected only by fair and lawful means without misleading or deceiving individuals/companies as to the reason.

- 4.3 The Officer shall ensure that the identifying purposes and consent principles are followed in identifying why personal information is being collected.

## **5 Limiting Use, Disclosure and Retention**

- 5.1 The Officer shall ensure that personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual/company or as required by law, and any use of personal information shall be documented appropriately.
- 5.2 The Officer shall ensure that all personal information is destroyed, erased, or made anonymous as soon as the purpose for which it was collected is no longer relevant or as permitted by law. There shall be an automatic review of the need to continue retaining personal information annually. Except as required to be kept by law, all personal information shall be deleted, erased, or made anonymous no later than five years after the purpose for which it was collected has been completed.
- 5.3 The Officer shall ensure that all use, disclosure and retention decisions are made in light of the consent principle, the identifying purposes principle and the individual access principle.

## **6 Accuracy**

- 6.1 The Officer shall reasonably ensure that the personal information is accurate, complete, and up to date, taking into account the individual's interests. The Officer shall ensure that the information is sufficiently accurate, complete, and up to date to minimize the possibility that inappropriate information might be used to decide on an individual.
- 6.2 The Officer shall ensure that Axiom does not routinely update personal information unless necessary to fulfil the purpose for which the information was collected.
- 6.3 The Officer shall ensure that personal information used on an ongoing basis, including information disclosed to third parties, should generally be accurate and up to date unless limits to the requirement for accuracy are set out.

## **7 Safeguards**

- 7.1 The Officer shall ensure Axiom has security safeguards to protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. The Officer shall do this regardless of the format in which Axiom holds the information.
- 7.2 Depending on the information's sensitivity, the Officer may permit reasonable discretion regarding the information that has to be collected: the amount, distribution, format, and storage method. A higher level of protection shall safeguard more sensitive information according to the consent principle's considerations.
- 7.3 The Officer shall ensure that the protection methods include:

- 7.3.1 Physical measures, for example, locked filing cabinets and restricted access to offices.
- 7.3.2 Organisational measures, for example, security clearance and limiting access on a "need-to-know" basis: and
- 7.3.3 Technological measures, for example, the use of passwords and information security.
- 7.4 The Officer shall ensure that all employees and volunteers know the importance of keeping personal information confidential.
- 7.5 The Officer shall ensure that care is taken when personal information is disposed of or destroyed to prevent unauthorized parties from gaining access to it.

## **8 Openness**

- 8.1 The Officer shall ensure that Axiom is open about its policies and practices regarding the management of personal information. The policies and information about the related practices shall be available without unreasonable effort in a generally understandable format.
- 8.2 The Officer shall ensure that the information available shall include,
  - 8.2.1 The name or title and address of the Officer who is accountable for Axiom policies and practices and to whom complaints or enquiries can be forwarded,
  - 8.2.2 The means of gaining access to personal information held by Axiom,
  - 8.2.3 A description of the type of personal information held by Axiom, including a general account of its use,
  - 8.2.4 A copy of any brochures or other information that explain Axiom policies, standards, or codes; and
  - 8.2.5 What personal information is made available to related organisations (e.g., organisations that are affiliated).
- 8.3 The Officer shall ensure the information that must be provided according to section 8.2 of this Policy and is available either in a brochure at the locations Axiom operates, online or through the mail.

## **9 Individual Access**

- 9.1 The Officer shall ensure that, upon request, Axiom shall inform an individual whether Axiom holds personal information about them. Axiom shall allow the individual access to the information. Axiom shall also account for the use that has been made or is being made of this information and give an account as to the third parties to whom it has been disclosed. (Note, if the Officer believes for valid reasons that access to personal information should be denied, the Officer shall consult legal counsel before making such a decision.) If possible, the information's source shall also be given.
- 9.2 The Officer may require a person requesting their personal information to give sufficient information to permit Axiom to provide an account of the existence, use and disclosure of personal information. Information shall be used only for the purpose for which it was obtained.
- 9.3 If Axiom has supplied personal information about an individual to third parties, the

Officer shall ensure that an attempt is made to be as specific as possible. When it is impossible to give a list of organisations to which Axiam disclosed information about an individual, Axiam shall provide a list of organisations to which it might have disclosed information about the individual.

- 9.4 The Officer shall ensure that Axiam responds to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be made available in a generally understandable form.
- 9.5 The Officer shall ensure that when an individual successfully demonstrates the inaccuracy or incompleteness of personal information, Axiam shall amend the information as required. Depending on the information challenged, amendment involves the correction, deletion, or addition of information in question.
- 9.6 The Officer shall ensure that when a challenge is not resolved to the individual's satisfaction, Axiam shall record the unresolved challenge's substance. When appropriate, the unresolved challenge's existence shall be transmitted to third parties having access to the information in question.

## **10 Challenging Compliance**

- 10.1 The Officer is authorized to address a challenge concerning compliance with the above principles.
- 10.2 The Officer shall develop procedures to receive and respond to complaints or enquiries about the policies and practices regarding the handling of personal information. The compliance procedures shall be easily accessible and straightforward to use.
- 10.3 The Officer shall inform individuals inquiring about lodging complaints that relevant complaint procedures exist.
- 10.4 The Officer shall investigate all complaints. If a complaint is found to be justified, the Officer shall take appropriate measures, including, if necessary, amending this Policy and general policies and practices about personal information entrusted to Axiam.