# PAIA and POPIA MANUAL

## M. PREM INCORPORATED

Prepared and published in accordance with the

Promotion of Access to Information Act, 2 of 2000, as amended,

and the Protection of Personal Information Act, 4 of 2013, as amended.

1. **Introduction**

**M Prem Incorporated** (the Company) recognises the constitutional rights of public and private bodies alike of access to information and privacy as enshrined in the Constitution of the Republic of South Africa, 1996. The Company acknowledges that it has a constitutional mandate to protect personal information pertaining to the relevant parties concerned.

This PAIA and POPIA Manual (the Manual) serves as a guide to promote, respect and protect the privacy of all persons who are associated with the Company whether as employees, business parties or other entities who are related to the Company.

2. **Background**

The Promotion of Access to Information Act, 2 of 2000 (PAIA) and the Protection of Personal Information Act, 4 of 2013 (POPIA) are both high reputational risk legislation that the Company has to comply with. The purpose of this legislation is to regulate the accessing and processing of personal information by public and private bodies.

3. **Purpose of this PAIA and POPIA Manual**

The purpose of this Manual is to incorporate the requirements of PAIA and the requirements of the POPIA into the daily operations of the Company and to ensure that these requirements are documented and implemented in the business processes.

3.1 The objective of this Manual is to ensure the constitutional right of access to information and the right to privacy with regard to:

3.1.1 the accessing of personal information;

3.1.2 the safeguarding of personal information;

3.1.3 the regulation and processing of personal Information;

3.1.4 the execution of prescribed requirement for the legal processing of personal information; and

3.1.5 the protection of free flow of personal information.

3.2 The Company and its employees shall adhere to this Manual concerning the management of all personal information received from, but not limited to natural

persons, employees, clients, suppliers, agents, representatives and partners of the Company, to ensure compliance is applied to these Acts and the applicable regulations and rules relating to the protection and accessing of personal information is adhered.

4. **Scope**

The contents of this Manual are applicable to all temporary and permanent employees of the Company, and has been introduced in order to encourage the protection and confidentiality of all personal information that has been made available to the Company by employees or any consumer/client or any party who has disclosed any information of a private or business nature, for the sole intention of employment, business transaction, contracts or communication and will be deemed to be necessary for the records pertaining of the Company

4.1 The Information Officer is the custodian of this Manual as it is the responsibility of the Information Officer to ensure that this Manual is incorporated and implemented in the various divisions of the Company, and that workshops training is provided to all parties concerned regarding the contents of PAIA and POPIA.

4.2 The Company will make employees and/or any parties aware of this Manual by discussing it during an induction session and by distributing it to the workforce by making it available and stored on the Company's electronic equipment. This Manual also applies to the processing of personal information entered in a record by making use of automated or non-automated means.

4.3 However, it remains the duty and responsibility of all employees and/or any parties to make themselves aware of, and to familiarise themselves with, the content and application of this document.

5. **Information Officer**

5.1 The Company appoints an Information Officer in terms of section 55 of the POPI Act.

5.2 This Manual is held by the Information Officer and, a copy can be requested from the Information Officer with the following details:

| | | |
|---|---|---|
| Information Officer | : | Monisha Prem |
| Designation | : | Managing Director |
| Telephone Number | : | 082 593 8262 |
| Email Address | : | monisha@mprem.co.za |

5.3 Any queries relating to this guide can be directed to:

The Information Regulator South Africa

| | | |
|---|---|---|
| Physical Address: | : | JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001 |
| Postal Address | : | P.O. Box 31533, Braamfontein, Johannesburg, 2017 |
| Telephone Number | : | 010 023 5200 |
| Website | : | www.justice.gov.za/inforeg/ |
| Email (General Enquiries) | : | inforeg@justice.gov.za |
| Email (Complaints) | : | complaints.IR@justice.gov.za |

## 6. Definitions

The following definitions apply to this Manual and is consistent with PAIA and POPIA. Any reference to the Acts refers to POPIA and PAIA.

| Concept | Definition |
|---|---|
| **Act** | Protection of Personal Information Act, 4 of 2013, as amended |
| **Automated** | Any equipment capable of operating automatically/independently in response to instructions being executed, for the purposes of processing information |
| **Code of Conduct** | Means a code of conduct issued in terms of Chapter 7 of the Act |
| **Company** | M. Prem Incorporated |
| **Conditions** | Conditions of Lawful Processing stipulated in Chapter 3 of the Act |
| **Constitution** | Constitution of the Republic of South Africa, 1996 |
| **Data Subject** | The person to whom the personal information is relative to including employees, customers, suppliers and or any third party |
| **De-identification** | Is the process used to prevent a person's identity from being connected with information |
| **Direct Marketing** | To approach/contact a Data Subject, either in person or by mail or electronic communication, for the direct or indirect purpose of – promoting or offering to supply, in the ordinary course of business, any goods or service to the Data Subject; or requesting a donation of any sort and for any reason from the Data Subject |
| **Employee** | An officially appointed person to any subsidiary in the M. Prem Incorporated, irrespective of the duration or nature of their appointment - permanent or temporary. |
| **Information Officer** | The head of a private body as contemplated in Section 1, contained in the Promotion of Access to Information Act (PAIA) |

| | |
|---|---|
| **Information Regulator** | The Information Regulator (South Africa) is an independent body established in terms of section 39 of the Act. The Information Regulator is responsible for protecting Data Subjects against harm and to ensure that their personal information is protected by responsible parties. |
| **Operator** | 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. |
| **PAIA** | Promotion of Access to Information Act, 2 of 2000, as amended |
| **Personal information** | 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, wellbeing, 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, 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 would reveal the contents of the original correspondence; the views or opinions of another individual regarding the person; and 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 |
| **POPIA** | Protection of Personal Information Act, 4 of 2013, as amended |
| **Process** | Means any operational activity concerning personal information including the collection, organisation, storage, modification, communication and destruction of information. |
| **Record** | Any recorded information in whatever form in possession or under the control of M. Prem Incorporated or any of its subsidiaries |
| **Responsible Party** | A public or private body or any other person which, independently or in conjunction with others, determines the purpose of and means for processing personal information (typically, but not always, the collector of information) |

7. **General provisions**

The right of access to information and the right to privacy are enshrined in the Constitution of the Republic of South Africa, 1996. PAIA is aimed at regulating access to personal information and records whilst POPIA is aimed at facilitating the processing of personal information.

7.1 This Manual establishes measures and standards for the protection and lawful processing of personal information within the Company and provides principles regarding the right of individuals to privacy and to reasonable safeguarding of their personal information.

7.2 The Company shall comply with both the law and good practice, respect individuals' rights to privacy, be open and honest with individuals whose data is held, provide training and support for staff who handle personal data, so that they can act confidently and consistently protect personal information and keeping information securely.

7.3 The Company acknowledges that it is mandatory to comply with the provisions of PAIA and POPIA.

8. **8 Conditions of the POPI Act**

POPIA places a responsibility on the Company to promote the lawful processing of personal information and its service providers who act on behalf of the Company. There are 8 (eight) Conditions that shall apply, and which are relevant for the lawful processing of personal information, namely:

8.1 **Processing Limitation**

8.1.1 The Company shall ensure that the processing of any personal information is done in accordance with the relevant legislation without infringing on the Data Subjects right to privacy; and

8.1.2 The Company shall ensure that personal information is only processed if the reasons given for the processing are adequate, legitimate, relevant and not excessive. Personal information shall be processed for the purpose it was collected for and not for a different purpose unless in accordance with exceptions in the Act.

8.2 **Specific purpose**

The Company shall only collect personal information for a specific purpose which is explicitly and limit the processing to the specific purpose it was collected for. The Company must ensure, in collecting the information, that the Data Subject is aware of the purpose for which the information is being collected.

8.3 **Further processing limitation**

The further processing of any personal information must be compatible with the purpose for which it was initially collected for.

8.4 **Information Quality**

The Company shall take reasonable steps to ensure that the personal information it processes, and stores is complete, accurate, not misleading and kept up to date where necessary.

8.5 **Openness**

8.5.1 The Company must maintain the documentation of all processing operations under its responsibility. The purpose of this condition is to ensure transparency and fairness in the processing of personal information; and

8.5.2 The Company shall ensure that the Data Subject is aware of the reasons for which his/her personal information is processed. The Company shall inform Data Subjects of any breaches relating to the Data Subject personal information.

8.6 **Security safeguards**

8.6.1 The Company shall secure the integrity and confidentiality of personal information in its possession through the implementation of appropriate measures to prevent; the loss, damage and unauthorised destruction of personal information; and unlawful access which leads to processing of personal information without the consent of the Data Subject; and

8.6.2 IT will guide the Company in terms of what are the appropriate IT security technologies to ensure safeguarding and protection of automated personal information and educate employees on protecting and securing automated processing of personal information;

8.6.3 IT will guide the Company in terms of appropriate security measures and facilities to ensure safeguarding and protection of non-automated personal information;

8.6.4 The Company shall also ensure that it has written agreements with all Operators processing personal information on its behalf. These agreements will need to outline the Operators measures to ensure the protection of personal information in their possession; and

8.6.5 The Company shall establish and implement processes or mechanisms to notify a Data Subject and the Information Regulator where there are reasonable grounds to believe that the personal information of a Data Subject has been accessed or acquired by any unauthorised person.

8.7 **Data subject participation**

The Company shall establish mechanisms and processes to provide Data Subjects with the opportunity to request, correct, delete or destroy their personal information insofar as requests have been done in the prescribed manner and where possible and justifiable.

9. **Further provisions**

9.1 **Personal Information Life Cycle**

9.1.1 Processing includes any activity concerning personal information. When employees, operators or the Company Subsidiaries:

9.1.1.1 Collects Personal Information;

9.1.1.2 Use Personal Information;

9.1.1.3 Share Personal Information;

9.1.1.4 Transfer Personal Information;

9.1.1.5 Store Personal Information; and

9.1.1.6 Destroy Personal Information;

shall do so in accordance with compliance requirements of the POPIA and PAIA Acts as well as this Manual.

10. **Further provisions**

10.1 **Additional rights and obligation not grouped under the 8 POPIA Conditions:**

10.1.1 Processing of special personal information;

10.1.2 Processing of Children's personal information;

10.1.3 Direct Marketing;

10.1.4 Processing subject to prior authorisation;

10.1.5 Profiling of Data Subjects based on the automated processing of personal information;

10.1.6 Transfer of personal information to other countries;

10.1.7 Notification to the Regulator;

10.1.8 Assessments;

10.1.9 Information Notices; and

10.1.10 Enforcement Notices and Administrative fines.

10.2 The Company shall take proper measures and controls to ensure compliance with these obligations.

11. **Training and Awareness**

Heads of Divisions shall ensure that all their staff members are trained on how to process personal information in accordance with the Act. The Information Officer shall be responsible to provide such training and general awareness.

12. **General Data Protection Regulation**

The Company must determine, based on its business model, if the Company activities falls within the ambit of the General Data Protection Regulation (GDPR). Based on the assessment if the GDPR applies to the Company, shall identify such activities, its risks and develop and monitor controls to minimise the risks associated with breach of GDPR.

13. **Notice in terms of Section 52(2) of PAIA read together with section 51(1)(c)**

No notice has been published by the Minister regarding the categories of records that are automatically available without formal request in terms of the Act.

14. **Processing of Personal Information**

The Company treats the privacy and protection of personal information held by it with utmost confidentiality and will only process the information in accordance with the privacy protection laws and principles of the Republic and in a manner that does not infringe on the Data Subject's rights.

14.1 The procedure of processing personal information refers to the collection, recording, organisation, storage, updating or modification, retrieval, consultation, use, dissemination by means of transmission, distribution or making available in any other form, erring, linking, including inaccessibility, erasure or destruction of personal information.

14.2 The information held by the Company is classified and grouped, without limitation, according to records relating to the following subjects:

| Subject | Category |
|---|---|
| Companies Act Records | Documents of Incorporation;<br>Index of names of Directors;<br>Memorandum of Incorporation;<br>Minutes of meetings of the Board of Directors;<br>Minutes of meetings of Shareholders;<br>Proxy forms;<br>Register of directors' shareholdings;<br>Share certificates;<br>Share Register and other statutory registers and/or records and/or documents;<br>Special resolutions/Resolutions passed at General and Class meetings;<br>Records relating to the appointment of:<br>Auditors;<br>Directors;<br>Prescribed Officer. |
| | Public Officer; and<br>Secretary |
| Financial Records | Accounting Records;<br>Annual Financial Reports;<br>Annual Financial Statements<br>Asset Registers;<br>Bank Statements;<br>Banking details and bank accounts;<br>Banking Records;<br>Debtors / Creditors statements and invoices; |

| | |
|---|---|
| | General ledgers and subsidiary ledgers;<br>General reconciliation;<br>Invoices;<br>Paid Cheques;<br>Policies and procedures;<br>Rental Agreements; and<br>Tax Returns |
| Income Tax Records | PAYE Records;<br>Documents issued to employees for income tax purposes; Records of payments made to SARS on behalf of employees;<br>All other statutory compliances:<br>VAT<br>Regional Services Levies<br>Skills Development Levies UIF<br>Workmen's Compensation |
| Personnel Documents and Records | Accident books and records;<br>Address Lists;<br>Disciplinary Code and Records;<br>Employee benefits arrangements rules and records;<br>Employment Contracts;<br>Employment Equity Plan;<br>Forms and Applications;<br>Grievance Procedures;<br>Leave Records;<br>Medical Aid Records;<br>Payroll reports/ Wage register;<br>Pension Fund Records;<br>Safety, Health and Environmental records; |
| | Salary Records;<br>SETA records<br>Standard letters and notices<br>Training Manuals;<br>Training Records;<br>Workplace and Union agreements and records. |
| Procurement Department | Standard Terms and Conditions for supply of services and products;<br>Contractor, client and supplier agreements;<br>Lists of suppliers, products, services and distribution; and Policies and Procedures. |
| Sales Department | Customer details |

| | |
|---|---|
| | Credit application information<br>Information and records provided by a third party |
| Marketing Department | Advertising and promotional material |
| Risk Management and Audit | Audit reports;<br>Risk management frameworks; and Risk management plans. |
| Safety, Health and Environment | Complete Safety, Health and Environment Risk Assessment<br>Environmental Managements Plans<br>Inquiries, inspections, examinations by environmental authorities |
| IT Department | Computer / mobile device usage policy documentation;<br>Disaster recovery plans;<br>Hardware asset registers;<br>Information security policies/standards/procedures;<br>Information technology systems and user manuals<br>Information usage policy documentation;<br>Project implementation plans;<br>Software licensing; and<br>System documentation and manuals. |
| Corporate Social Responsibility (CSR) | CSR schedule of projects/record of organisations that receive funding; Reports, books, publications and general information related to CSR spend;<br>Records and contracts of agreement with funded organisations. |

14.3 Personal information collected by the Company and/or any of its representatives or subsidiaries, will not be collected directly from the Data Subject, unless:

14.3.1 The information is contained or derived from a public record or has deliberately been made public by the Data Subject;

14.3.2 The Data Subject or a competent person where the Data Subject is a minor, has consented, to the collection of the information from another source;

14.3.3 Collection of the information from another source would not prejudice a legitimate interest of the Data Subject;

14.3.4 Collection of the information from another source is necessary to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences; to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue; for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; in the interest of national security; or to maintain the legitimate interests of the Company or of a third party to whom the information is supplied;

14.3.5 Compliance would prejudice a lawful purpose of the collection; or

14.3.6 Compliance is not reasonably practicable in the circumstances of that instance.

14.4 Personal information must only be collected for a specific, explicitly, defined and lawful purpose, related to the function or activity of the Company.

14.5 Ensure that the Data Subject is aware of what information is collected prior to the collection thereof.

14.6 Ensure the Data Subject, or should the individual be a minor, a competent person in this instance then consents to the collection of personal information.

14.7 Inform the Data Subject what the purpose is for the collection of this information and inform the Data Subject regarding:

14.7.1 whether the information to be collected is a voluntary or mandatory function to be performed; the consequences of the matter for the Data Subject should they fail to provide the information; whether it is ascertained that a legal authority requires the collection of the information for their records;

14.7.2 whether this information needs to be transferred to another source; and

14.7.3 whether the Company intends to transfer the information to any other country outside the borders of the Republic of South Africa or international organisation and disclose the level of protection regarding the personal information which can be expected from this country or international organisation.

14.8 Ensure that the personal information is complete, accurate, not misleading and is updated from time to time.

14.9 Ensure that the information which is collected is not excessive. To collect solely the information which is necessary for the company, which it requires to execute its functions or in the interests of a third party, where the information will be provided to them.

14.10 To undertake to regard personal information as strictly private and confidential and not to disclose it to any other party, unless required by law to take this course of action, or the consideration of the correct performance of the company's duties and tasks.

14.11 The Company will take responsibility to keep on record all the appropriate documentation of all processing operations.

## 15. Retention and restriction of records

15.1 Records of personal information should not be retained for longer periods than is necessary for achieving the purpose for which the information was collected, unless:

15.1.1 the retention of a record is required or authorised by law;

15.1.2 the Company reasonably requires a record for legal purposes related to its functions or activities;

15.1.3 retention of a record is required by a contract between the parties thereto; or

15.1.4 the Data Subject or a competent person where the Data Subject is a minor and has consented to the retention of a record.

15.2 The Company will destroy or delete a record of personal information as soon as it is reasonably practical once it has no further authority to retain a record for a further period.

15.3 The deletion of a record of personal information should be processed in a manner that prevents its reconstruction in an intelligible/understandable form.

15.4 In the event where the Company uses a record of personal information from a Data Subject to arrive at a conclusion regarding various aspect pertinent to the Data Subject, the following will be necessary:

15.4.1 Retain the record for such period as may be required or prescribed by law or a code of conduct; or

15.4.2 If there is no law or code of conduct prescribing a retention period, retain the record for a period that will afford the Data Subject a reasonable opportunity in which to request access to the record, taking all considerations relating to the use of the personal information into account.

15.5 The Company will restrict the processing of personal information if:

15.5.1 its accuracy is contested by the Data Subject, for a period enabling the Company to verify the accuracy of the information;

15.5.2 the Company no longer requires the personal information for achieving the purpose for which it was collected or subsequently processed, but is required to maintain/retain it for purposes of proof or record keeping purposes;

15.5.3 the processing is unlawful, and the Data Subject opposes its destruction or deletion and alternatively requests the restriction of its use; or

15.5.4 the Data Subject requests that the personal data be transmitted or transferred to another automated processing system.

15.6 Personal information that has been restricted may only be processed for purposes of proof, or processed with the Data Subject's consent, or with the consent of a competent person where the Data Subject is a minor, or for the protection of the rights of any other natural or legal person, or if such processing is in the public interest.

15.7 Where personal information is restricted, the Company will inform the Data Subject prior to the termination of the restriction.

## 16. Security safeguards

16.1 The Company will secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable, technical and organisational measures to prevent loss of, damage to, or unauthorised destruction of personal information; and unlawful access to or processing of personal information.

16.2 The Company will take responsible measures to:

16.2.1 identify all reasonable predictable internal and external risks to personal information in its possession or under its management;

16.2.2 establish and maintain appropriate safeguards against the risks identified;

16.2.3 regularly verify that the safeguards are effectively implemented; and

16.2.4 ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguarding methods.

16.3 The Company will have due regard to generally accepted Information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

## 17. Security Compromises

17.1 Where there are reasonable grounds to believe that the personal information of a Data Subject has been accessed or acquired by any unauthorised person, the Information Officer should be contacted immediately.

17.2 The Information Officer is required to notify the information regulator and the Data Subject.

17.3 The notification of a breach of confidentiality should be declared as soon as is reasonably possible upon the discovery of the compromise.

17.4 The Information Officer needs to provide sufficient information to the Data Subject which will enable the Data Subject to take protective measures against the potential consequences of the compromise.

17.5 The Company is entitled to refuse a request for information to uphold the mandatory protection of the privacy of Data Subjects.

17.6 Where confidential and personal records of third parties will unreasonably be disclosed, permission from the Data Subject concerned will be sought, in addition to normal requirements, before the Company will consider access.

## 18. Rights of the Data Subject

18.1 The Data Subject, or competent person where the Data Subject is a minor, may withdraw his, her or its consent to procure and process his/her or its personal information, at any time, providing that the processing of the personal information was performed legally, prior to the request for the withdrawal.

18.2 A Data Subject, having provided adequate proof of identity, has the right to:

18.2.1 request the Company to confirm, free of charge, whether it holds personal information regarding the Data Subject; and

18.2.2 request from the Company a record or a description of the personal information relevant to the Data Subject held by the Company, including information regarding the identity of all third parties, or categories of third parties, who have, or have had, access to the information.

18.3 This must be processed within a reasonable period, at a fee prescribed as determined by the Information Officer, in a reasonable manner and format and in a form that is generally understandable.

18.4 A Data Subject may request the Company, to correct or delete personal information in its possession or under its management which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or has been obtained illegally.

18.5 A Data Subject may request the Company to destroy or delete their record of personal information. This must be processed only if it is permissible and has been approved by the Information Officer.

## 19. Monitoring and enforcement

19.1 All employees will be responsible for administering and overseeing the implementation of this Manual including the supporting of guidelines, standard operating procedure, notices, consents and appropriate related documents and processes.

19.2 Employees who violate the guidelines and standard operating procedures of this Manual may be subjected to disciplinary action, being taken against him/her.

19.3 The point of contact for requests, disclosures, questions, complaints and any other inquiries relating to the processing, collection, or re-identifying of personal information shall be directed to the Information Officer or Deputy Information Officer(s).

## 20. Prescribed request procedure

20.1 A request for access to a record or information must be made on the prescribed form and addressed to the Information Officer.

20.2 Any request which does not comply with the formalities as prescribed by PAIA will be returned to the requester concerned.

20.3 The requester must complete the form concisely with sufficient detail to enable the Information Officer to identity the record and the requester.

20.4 The requester must identify the right sought to be exercised or to be protected and provide an explanation why the requested record is required for the exercise of the protection of that right.

20.5 The requester should indicate if it wishes to be informed of the decision of the Information Officer in any other manner (in addition to writing).

20.6 Where a request is made on behalf of another person, the requester must submit proof of his/her capacity to make the request on behalf of another person.

21. **Fees**

21.1 The requester is required to pay the prescribed fee of R50.00 (Fifty Rand) before the processing of a request, which fee may be waived at the discretion of the Information Officer. Fees in respect of private bodies can be obtained from the Information Officer or his deputy.

21.2 The Information Officer must inform the requester in writing of the decision of the request.

21.3 Where a decision to grant a request has been taken, the Information Officer must, by notice, require the requester to pay the necessary fees in full before the records are processed.

21.4 Records may be withheld until the fees have been paid in full.

22. **Objection**

22.1 A Data Subject may, at any time, on reasonable grounds, object to the processing of personal information by the Company unless legislation provides for the processing of such information.

22.2 Where a Data Subject objects to the processing of personal information, it must complete the prescribed form and submit it to the Information Officer.

23. **Remedies**

23.1 The Company does not have internal appeal procedures regarding PAIA and POPIA requests and as such, the decision made by the duly authorised persons in paragraphs 5 above are final.

23.2 A party that is dissatisfied with the decision of the duly authorised persons may within 30 (thirty) days of notification of the decision apply to a Court with competent jurisdiction for relief.