EERSTE | FLAMBEAU

HUUR (PTY)LTD

HUMAN RESOURCES POLICIES & PROCEDURES

Subject:	Protection of Personal Information Policy		Pages: 14
Controlled by:	Group Human Resources & Legal		Document No. 01
Approved by:	Board of Directors		
NEW POLICY	✓	Effective Date: 1 September 2021	
REVISION		Review date: 1 September 2023	

1. RELEVANT DEFINITIONS

These definitions are taken from the Promotion of Access to Information Act 2 of 2000 as amended (PAIA) and the Protection of Personal Information Act 4 of 2013 (POPIA).

"Body" means a public or private body;

"Data Subject" means the person to whom personal information relates.

"Group" means the Eerste Falmbea Huur (PTY) Ltd and its subsidiaries, Glodina Towelling (PTY) Ltd and Colibri Towelling Western Cape (PTY) Ltd.

"Head" of, or in relation to, a private Body means –

(a) in the case of a natural person, that natural person or any person duly authorised by that natural person;

(b) in the case of a partnership, any partner of the partnership or any person duly authorised by the partnership;

(c) in the case of a juristic person –

(i) the chief executive officer or equivalent officer of the juristic person or any person duly authorised by that officer; or

(ii) the person who is acting as such or any person duly authorised by such acting person.

"Information Officer": of, or in relation to, a –

(a) public body means an Information Officer or Deputy Information Officer as contemplated in terms of section 1 or 17 of the Promotion of Access to Information Act; or Page 4 of 29 b) private body means the head of a private body as contemplated in

section 1 of the Promotion of Access to Information Act.

"Person" means a natural person or a juristic person.

"Personal Information" – means information relating to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person, including, but not limited to —

(a) 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;

(b) information relating to the education or the medical, financial, criminal or employment history of the person;

(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

(d) the biometric information of the person;

(e) the personal opinions, views or preferences of the person;

(f) 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;

(g) the views or 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.

"Private Body" means –

(a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity.

(b) a partnership which carries or has carried on any trade, business or profession; or

(c) any former or existing juristic person, but excludes a public body.

"Processing" means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including —

(a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

(b) dissemination by means of transmission, distribution or making available in any other form; or

(c) merging, linking, as well as restriction, degradation, erasure or destruction of

information.

"Public Body" means –

(a) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or

(b) any other functionary or institution when

(i) exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or

(ii) exercising a public power or performing a public function in terms of any legislation.

"Requester", in relation to –

(a) a public body, means –

(i) any person (other than a public body contemplated in paragraph (a) or (b)

(i) of the definition of 'public body', or an official thereof making a request for access to a record of that public body; or

(ii) a person acting on behalf of the person referred to in subparagraph (i).

(b) a private body, means –

(i) any person, including, but not limited to, a public body or an official thereof, making a request for access to a record of that private body; or

(ii) a person acting on behalf of the person contemplated in (i).

''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;

2. BACKGROUND

2.1 Section 14 of the Constitution of the Republic of South Africa, 1996 (Constitution) provides that everyone has the right to privacy. This includes a right to protection against unlawful collection, retention, dissemination and use of personal information (PI). The Constitution recognizes that the processing of personal information constitutes a threat to one's right to privacy and right to protect one's identity. The right to privacy can be infringed by the unauthorized collection and disclosure of PI.

2.2 To encourage the protection of PI processed by both public and private bodies, the

South African Government signed into law the Protection of Personal Information Act 4 of 2013 (POPIA). It gives expression to the constitutional values of democracy and openness, recognising the need for economic and social progress within the framework of the information society and the need for removal of unnecessary impediments to the free flow of information. POPIA has been promulgated to regulate, in harmony with international standards, the processing of PI in a manner that gives effect to the right to privacy subject to justifiable limitations that are aimed at protecting other rights and important interests.

2.3 POPIA recognises the right to privacy as enshrined in the Constitution and gives effect to this right by introducing certain conditions that establish the minimum requirements that businesses need to comply with when processing personal information of natural and juristic persons. Accordingly, POPIA covers all information and/or data that private and public bodies collect, retain or archive on both their clients and/or prospective clients as well as individuals who work; might wish to work or has worked for such bodies.

2.4 The Group is committed to protecting the right to privacy of all its data subjects as well as fostering a culture of transparency and accountability. To demonstrate this balance, the corporation will be guided by this POPI policy which provides directive on how PI and data will be processed in accordance to the prescripts of the Protection of Personal Information Act 4 of 2013.

2.5 The policy will dovetail with all other information and data policies as well as align with the Groups organisational systems and procedures. In an event that there be cases where a conflict occurs between the POPI policy directives with any other information and data policy; the protection of personal information provisions under the POPIA will prevail, unless the other law gives greater protection of personal information.

3. INTRODUCTION

3.1 The Group as an employer processes PI of current, former, and prospective employees. Given the importance of privacy, the organization is committed to effectively manage such information in accordance with POPIA's provisions.

3.2 Much of the PI, that is collected, stored and processed by the Group is in the form of electronic data and in hard copy documents. POPIA requires that such information be captured, kept, and classified and maintained in the following manner:

- Only that which is relevant for the purpose;
- Only be retained for maximum prescribed period as may be applicable;
- Integrity and confidentiality to always be maintained, and
- Used only for the purpose for which it was collected for.

By adopting this policy, the Group shall ensure the preservation of PI from commencement of the relationship to its termination, considering the applicable data retention principles.

4. PURPOSE & SCOPE OF THE POLICY DOCUMENT

4.1 Purpose

The purpose of this policy document is to provide a high-level statement in respect of the Groups approach to the adoption and implementation of POPIA to achieve the following:

- Facilitate compliance with POPIA and applicable regulatory requirements relating to protection of PI applicable from time to time;
- State the desired behavior and direct compliance with the provisions of POPIA;
- Cultivate an organisational culture that recognizes privacy as a valuable human right;
- Direct and provide guidance towards development and implementation of internal controls for the purpose of managing compliance risk associated with the protection of personal information;
- Promote business practices that will provide reasonable assurance that rights of data subjects are protected and balanced with the legitimate business needs of the corporation;
- Reflect specific duties and responsibilities for responsible parties including the appointment of an Information Officer and Deputy Information Officer to

protect the interest of the corporation and data subjects.

The policy will mitigate against the risks associated with protection of information failures which include:

- **Breaches of confidentiality** which may result in revenue penalties (loss in revenue where if found guilty of non-compliance).
- **Failing to obtain prior consent** which may result in a complaint to the Information Regulator or a civil proceeding instituted by the data subject;
- **Reputational damage** – the Group may suffer financial and/ or reputational damages if found non - compliant following an adverse event like hacking which results in PI being compromised.

4.2 Scope

The legal duty to comply with the POPIA provisions is activated in any situation where there is processing, or personal information is entered into a record by or for a responsible person who is domiciled in South Africa.

Adherence to the policy applies therefore to all staff members, all subsidiaries, including contractors and part time employees in situation where they collect and /process personal information as classified by the POPIA.

POPIA does not apply in situations where the PI has been de-identified.

5. POLICY STATEMENT

5.1 Commitment to Compliance

Whereas the Group recognizes the importance of safeguarding and maintaining the confidentiality of PI collected, stored and/or processed. Now therefore, it commits to comply with both the spirit and letter of applicable regulatory requirements and to always act with due care, skill, and diligence when processing PI.

6. RATIONALE

6.1 The Group takes its obligation to comply with applicable laws, rules regulations and standards extremely seriously, including the spirit of the law. Therefore, the importance of complying with the ever-changing legislative developments and the implementation of effective regulatory compliance risk management structures, processes and procedures is imperative for the Group.

6.2 It is recognized that the Board, the Group as employer/ accountable institution [including Executive Management, Line Management, and all employees] including all subsidiaries and contractors in their individual and collective capacity, could potentially be exposed to regulatory fines, sanctions, penalties, civil claims as well as reputational damage as a result of non - compliance with applicable regulatory requirements. Thus, it is important that everyone understand their respective roles/ responsibilities as well as any applicable repercussions in the event on non-compliance.

6.3 Compliance is of paramount importance in attaining and maintaining corporate integrity with clients (internal and external). Failure to comply with applicable regulatory requirements will threaten the status of the Group as a reliable, honest, and trustworthy corporate.

7. GUIDING CONDITIONS FOR PROCESSING PERSONAL INFORMATION

All employees and persons acting on behalf of the Group will at all times adhere to the eight conditions as prescribed by the POPIA when processing personal information of natural and juristic persons, clients and or prospective clients as well as employees; prospective and former employees.

7.1 Accountability

The Group will ensure that the provisions of POPIA, the guiding principles outlined in the policy and all the measures that give effect to such provisions are complied with at the time of the determination of the purpose and means of the processing and during the processing itself. In the event that an employee of the Group or any person acting on

behalf of the Group who through their intentional or negligent actions and/or omissions fail to comply with the principles and responsibilities outlined, proper punitive measures will be applied.

7.2 Purpose Specification

All Group business units and departments will process personal information only for specific, explicitly defined, and legitimate reasons. The Group will inform data subjects of reasons prior to collecting or recording their PI.

7.3 Further Processing Limitation

Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose. Thus, where the Group seeks to process personal information, it holds for a purpose for which it was originally collected, and where this secondary purpose is not compatible with the original purpose, the organisation will first obtain additional consent from the data subject.

7.4 Information Quality

The Group will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading. Where PI is collected or received from third parties, the corporation will 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.

7.5 Open Communication

Reasonable steps will be taken by the Group to ensure that data subjects are notified of the purpose for which the information is being collected, used, and processed. Through the Group notified communication channels, data subjects will be entitled to make enquiries pertaining to their PI including, but not limited to:

7.5.1 access to their PI stored by the Group

7.5.2 provide updates, corrections or request the deletion of their PI subject to

applicable Group retention policies, from time to time

7.5.3 Lodge a complaint concerning processing of their PI.

7.6 Security Safeguards

The Group will secure the integrity and confidentiality of PI in its possession or under its control by taking appropriate, reasonably, technical and organizational measures to prevent loss of, damage to or unauthorized destruction of PI and unlawful access to or processing of personal information. These controls will continuously be reviewed and include regular monitoring of the adopted systems and procedures as well as testing of protocols and measures applied to combat cyber-attacks on the corporation's IT networks.

7.7 Data Subject Participation

A data subject whose PI has been collected, stored, and processed by the Group may request for the correction or deletion of such information. The Group will encourage data subjects to use the current communication channels to make such requests.

7.8 Processing Limitations

The processing of personal information by the Group must at all times be lawful and done in a reasonable manner to ensure that the privacy of a data subject is not infringed when personal information is being processed. In order to ensure that the privacy of the data subject is not infringed, the Group will adopt a purpose for processing that is adequate, relevant, and not excessive.

8 RIGHTS OF DATA SUBJECT

Where appropriate, the Group will ensure that its clients and employees are made aware of the rights conferred upon them as data subjects. The Group will ensure that it gives effect to the following rights:

8.1 The Right to access PI

The Group recognizes that a data subject has the right to enquire regarding the PI that the Group might hold PI in relation to the data subject, including access requirements.

8.2 **The Right to have PI Corrected or Deleted**

The data subject has the right to request, where necessary; that his, her or it's PI must be corrected or deleted where the organisation is no longer authorised to retain the PI. [*Personal Information Request Form attached as Annexure a*].

8.3 **The Right to Object to the Processing of PI**

The data subject has the right, on reasonable grounds, to object to the processing of the PI. In such instances the Group will give due consideration to the request and the requirements of the POPIA.

The Group may cease to use or disclose the data subject's PI and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of the PI, subject to retention policy as applicable from time to time.

8.4 **The Right to Object to Direct Marketing**

The data subject has the right to object to the processing of the PI for purposes of direct marketing by means of unsolicited electronic communications.

8.5 **The Right to Complain to the Information Regulator**

The data subject has the right to submit a complaint to the Information Regulator regarding the alleged infringement of any of the right protected under the POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of the PI.

8.6 **The Right to be Informed**

The data subject has the right to be notified that the PI is being collected by the Group. The Group, as a Responsible Party will endeavor to inform the data subject of any situation where there are reasonable grounds to believe that the PI of the data subject has been accessed or acquired by an unauthorised person.

9 RESPONSIBILITIES OF ROLE PLAYERS

9.1 Board of Directors

The Board of Directors (BoD) is accountable to lead, control and monitor the business activities of the Group and provide effective corporate governance with the responsibility to oversee compliance with regulatory requirements. Thus, it is ultimately accountable for regulatory compliance within the Group.

9.2 Executive Management

The Group's Executive and Management is delegated the responsibility to ensure that all Group business activities are conducted in compliance with all the applicable regulatory requirements. Thus, it is imperative that there must be an appropriate focus on developing and maintaining an effective regulatory compliance risk management framework, process, and systems within the Group.

9.3 Line Managers

They are responsible for the regulatory compliance risks within their respective departments. Their responsibility regarding compliance includes the implementation of compliance procedures to ensure adherence to statutory and supervisory requirements and to ensure that such processes and procedures are carried out effectively within their departments.

9.4 External Auditors

The External Auditors play an assurance role by reviewing the existence and adequacy of control systems to ensure proper compliance with laid down policies, compliance risk

management frameworks, compliance processes and procedures, supervisory and regulatory requirements.

9.5 **Information Officer and Deputy Information Officer**

Information Officers are, by virtue of their positions, appointed automatically in terms of the PAIA Act and POPI Act respectively. The position is automatically assigned to the head of an organisation (CEO).

POPIA, in terms of its Section 56 read together with the provisions of Section 17 of PAIA, provides for the delegation of authority through the appointment of deputy information officers, to assist the information officer with the performance of his or her responsibilities and duties towards the responsible party, and the proper fulfilment of his or her mandate.

The Information Officer and Deputy Information Officer will be registered with the South African Information Regulator established under POPIA prior to performing his or her duties. These duties include, but are not limited to:

9.5.1 Encourage and ensure overall compliance with the provisions of POPIA

9.5.2 Keep the governing body updated about the corporation's information protection responsibilities under POPIA.

9.5.3 Work with the Regulator in relation to investigations conducted in accordance with the relevant provisions of POPIA;

9.5.4 Ensure that a personal information impact/risk assessment is performed to guarantee that adequate measures and standards exist within the entity;

9.5.5 Ensure that internal awareness sessions are conducted regarding the provisions of POPIA, the regulations and any codes of conduct or information obtained from the Regulator.

9.6 **All Employees**

All employees within the Group share the responsibility for compliance regardless of their position within the group. Therefore, all employees are responsible for conducting all business activities in compliance with applicable regulatory requirements.

10 ACTIONS FOR NON- COMPLIANCE

10.1 Non-compliance with the POPIA regulatory requirements in respect of the processing of personal information will be seen in a very serious light. Thus, in instances of non-compliance a remedial action will be addressed in line with the Group's disciplinary processes and procedures.

11 SURVEILLANCE SYSTEMS

11.1 Video footage and/or voice/telephone calls that have been recorded, processed and stored via CCTV camera or other surveillance systems constitute personal information. As such the Group will make all employees, members, clients or data subjects aware as to the use of CCTV/other surveillance on the premises.

12 CLEAN DESK

12.1 The purpose for this clause is to establish a culture of security and trust for all employees. An effective clean desk effort involving the participation and support of all employees can greatly protect paper documents that contain sensitive information about our clients, customers and vendors. All employees should familiarize themselves with the guidelines of this policy.

12.2 The main reasons for a clean desk policy are:

12.2.1 A clean desk can produce a positive image when our customers visit the sites.

12.2.2 It reduces the threat of a security incident as confidential information will be locked away when unattended.

12.2.3 Sensitive documents left in the open can be stolen by a malicious entity.

12.3 At known extended periods away from your desk, such as a lunch break, sensitive working papers are expected to be placed in locked drawers.

12.4 At the end of the working day the employee is expected to tidy their desk and to put

away all office papers. The Group provides filing cabinets for this purpose.

12.5 The following recommendations will be communicated to all employees:

12.5.1 Allocate time in your calendar to clear away your paperwork.

12.5.2 Always clear your workspace before leaving for longer periods of time.

12.5.3 If in doubt - throw it out. If you are unsure of whether a duplicate piece of sensitive documentation should be kept - it will probably be better to place it in the shred bin.

12.5.4 Consider scanning paper items and filing them electronically in your workstation.

12.5.5 Lock your office and filing cabinets at the end of the day

12.5.6 Lock away portable computing devices such as laptops or PDA devices

12.5.7 Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer

APPROVAL

Naeem Timol
Group HR & Legal

22 October 2021
Date

Abdul Gakeem Satira
Chief Executive Officer

26 November 2021
Date