Group Privacy Policy

Classification	INTERNAL		
Document Type	Policy		
Policy Reference Number	BW-GRP-LEG-002		
Area of Applicability	Barloworld Group		
Policy Owner	Group General Counsel – Sandile Langa		
Policy Owner Contact Information	Sandile.Langa@barloworld.com		
Version	V2.0		
Date Approved	20 May 2022		
Approved by	Group Executive Committee Group Risk Committee		
Policy Sponsor	Group Company Secretary – Nomini Rapoo		
Effective Date	20 May 2020		
Next Review Date	December 2023		
Documentation Status	☐ Working draft	☐ Consultation Release	☐ Final version

APPROVAL AND OWNERSHIP

Policy Owner	Date
Group General Counsel – Moipone Khojane	Sep 2019
Group General Counsel – Sandile Langa	Aug 2022

Approved By	Date
Group Executive Committee	28 Mar 2022
Group Risk Committee	20 May 2022

REVISION HISTORY

Version	Revision Date	Description	Next review Date
V1.0	Sep 2019	New policy developed to support POPIA / PAIA compliance.	Dec 2021
V2.0	May 2022	Revision of Privacy Policy to address audit findings and align with local and international Privacy standards and best practices.	May 2024

Contents

DEFINITIONS AND ABBREVIATIONS

Table 1: Definitions

Terminology	Description
Barloworld	Barloworld means Barloworld Limited and its subsidiaries, divisions and business units in all countries in which it does business, or any individual subsidiary in its own capacity. For purposes of this Policy, Barloworld may also be referred to as the "Group". It does not include joint ventures, other than those where Barloworld exercises management control, nor does it include investments where Barloworld owns less than 50%.
Binding Corporate Rules	means Personal Information processing policies, within a group of undertakings, which are adhered to by a responsible party or Operator within that group of undertakings when transferring Personal Information to a responsible party or Operator within that same group of undertakings in a foreign country; and "group of undertakings" means a controlling undertaking and its controlled undertakings. In certain foreign jurisdictions, Binding Corporate Rules must be approved by a supervisory authority. There is no approval requirement for this under POPIA, as applicable in South Africa.
Data	means Information, which is recorded in any format, whether stored electronically or in a paper-based form. For purposes of this Policy, the terms Data and Information may be used interchangeably.
Deputy Information officer	a Barloworld Employee to whom the Information Officer has delegated their powers and duties in terms of POPIA to support them in ensuring compliance with POPIA and PAIA within a division / legal entity. This constitutes a statutory appointment in accordance with POPIA and PAIA and is registered with the Information Regulator (in South Africa)
Employee	means an individual holding a permanent or fixed-term contract of employment within Barloworld.
Information	means Data which is processed, captured, stored and/or transmitted on Information systems or in paper-based form regardless of the media used.
Information Officer	a Barloworld Employee appointed to ensure compliance with POPIA and PAIA within a division / legal entity. This constitutes a statutory appointment in accordance with POPIA and PAIA and is registered with the Information Regulator (in South Africa).
Information Regulator	refers to the independent regulatory body in South Africa, established in terms of S39 of POPIA, with legislated authority to enforce and monitor compliance to POPIA and PAIA, including the investigation of reported privacy breaches.
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 that party, such as call centres, outsourced payroll administrators, document management warehouses and persons who clear the payment instructions of Barloworld's customers.
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, well-being, disability, religion, conscience, belief, culture, language and birth of the person; • Information relating to the education or the medical, financial, criminal or employment history of the person; • any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; • the biometric information of the person; • the personal opinions, views or preferences of the person; • correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; • the views or opinions of another individual about 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.
Privacy	means the right to be left alone, whereby one is free from interference and intrusion.
Processing	any operation or activity whether or not by automatic means, concerning Records including collecting, receiving, recording, organising, collating, storing, updating, modifying, retrieving, altering, consulting or using, disseminating, distributing or making available and merging, linking, blocking, degrading, erasing, destroying Records.
Record	any recorded Information, regardless of form or medium, including any of the following: • writing on any material; • Information produced, recorded or stored by means of any tape recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from Information so produced, recorded or stored; • label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means; • book, map, plan, graph or drawing; • photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced; • in the possession or under the control of Barloworld; • whether or not it was created by Barloworld; • and regardless of when it came into existence
South Africa	means the Republic of South Africa.
Special Personal Information	means Personal Information that relates to: a) 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 b) the criminal behaviour of a Data Subject to the extent that such Information relates to-

	(i) the alleged commission by a Data Subject of any offence; or (ii) any proceedings in respect of any offence allegedly committed by a Data Subject or the disposal of such proceedings.

Table 2: Abbreviations

Abbreviation	Description
Divisional CEO	Chief Executive Officer of a particular Division
Group CEO	Group Chief Executive Officer
Group FD	Group Finance Director

1 Preamble and Policy Summary

Barloworld values the right to Privacy as being intrinsic to its core values and embedded in its business practices. The evolving global Privacy regulatory landscape means that organisations such as Barloworld must comply with applicable Personal Information / Data protection laws and regulations relating to privacy in countries where it operates.

In South Africa, the Protection of Personal Information Act, 04 of 2013, ("POPIA") became largely effective on 01 July 2021 and, generally, regulates the processing of all individual and juristic / corporate Personal Information within South Africa, in support of the constitutional right to Privacy. POPIA must be read in conjunction with the Promotion of Access to Information Act, 2 of 2000 ("PAIA"), applicable in South Africa, which enables third parties to make application to a legal entity to obtain access to certain Records and Information.

Due to the extent of operations across the Barloworld Group, this Group Privacy Policy ("this/the Policy) seeks to align with local and international privacy laws and recognised best practices relating to privacy and Data protection.

2 Purpose and Objective

Barloworld Processes Personal Information of Data Subjects to promote and facilitate business transactions. Such Processing exposes Data Subjects to risks such as loss, theft, unauthorised access, or accidental disclosure of their Personal Information.

This can result in fines, reputational damage and / or other legal liabilities for Barloworld in terms of applicable Data protection and privacy laws.

The purpose of this Policy is to ensure that the Processing of Personal Information by or on behalf of Barloworld is done in accordance with applicable privacy and Data protection laws. While this Policy has been based on the requirements of POPIA, all legal entities operating outside of South Africa must ensure compliance with all local privacy and Data protection laws.

To the extent that there may be material differences between the requirements of this Policy and those of locally applicable privacy / Data protection laws, the application of local laws will prevail, subject to consultations with the Group / divisional Information Officer. Where a legal entity may not be governed by any privacy / Data protection laws, then this Policy and the Group Privacy Framework will apply as Corporate Binding Rules.

3 Scope

This policy is applicable to all Barloworld officers, directors, Employees, agents, contractors, consultants, advisors or suppliers who are involved in the Processing of Personal Information for / on behalf of Barloworld.

This Policy covers Personal Information Processed specifically for authorised Barloworld business activities. Any Personal Information held by Barloworld which is Processed for purposes unrelated to Barloworld business activities, or for personal purposes, is strictly prohibited, and anyone who Processes Personal Information held by Barloworld for personal reasons unrelated to Barloworld business, will become personally responsible and liable for such use, including any breaches arising therefrom.

4 Roles and Responsibilities

Divisional executive management have the responsibility to ensure compliance with this Policy and the discretion to define additional supporting processes, procedures, and other mechanisms by which the Policy is implemented. All divisions and legal entities must ensure that they have appointed an Information Officer and deputy Information Officer to facilitate and oversee the implementation of this Policy and the Barloworld Group Privacy Framework.

5 Regulatory Background

Barloworld adheres to global privacy standards and best practices and has based this Policy on the conditions for lawful processing of Personal Information as set out in Chapter 3 of POPIA (“Processing Conditions”).

Anyone Processing Personal Information on behalf of Barloworld must comply with the following eight (8) Processing Conditions (as amended / supplemented by mandatory provisions of applicable / equivalent local privacy and Data protection laws). A detailed explanation of these eight (8) conditions for lawful Processing of Personal Information is more fully set out in the Group Privacy Framework.

Condition 1: accountability.

Condition 2: Processing limitation.

Condition 3: purpose specification.

Condition 4: further Processing limitation.

Condition 5: information quality.

Condition 6: openness.

Condition 7: security safeguards.

Condition 8: Data Subject participation.

6 Policy Statement

6.1 Privacy Governance

The Group Privacy Steering Committee is a governance oversight committee chaired by the Group Information Officer and reporting into the Barloworld Group Executive Committee. Its mandate is to implement a cross-functional and cross-divisional privacy operating model as defined in the Barloworld Group Privacy Framework across the Barloworld Group to ensure compliance with applicable privacy and Data protection laws and is the custodian of this Policy.

The Group Privacy Framework serves a as a standard operating model regulating privacy compliance within the Group. It is a consolidated set of Corporate Binding Rules, operating procedures and business processes which serves as a complementary supporting framework to this Policy. Both this Policy and the Group Privacy Framework must be implemented by the respective divisions / legal entities to give effect to the principles contained in this Policy. Divisions / legal entities will be monitored for their compliance toward this Policy and the Group Privacy Framework and will be required to report on their status of compliance to the Barloworld Group Privacy Steering Committee and any other divisional oversight committees.

6.2 Managing Privacy Incidents

Privacy incidents may occur for various reasons, notwithstanding all reasonable precautions that may be in place. A privacy incident occurs when there are reasonable grounds to believe that a loss of control, compromise, unauthorised disclosure, acquisition, access, to Personal Information or Special Personal Information occurred and may occur where persons who are not authorised users have access or potential access to Personal Information or Special Personal Information, whether physical or electronic.

If an Employee becomes aware of a privacy incident, they must report it to the relevant Information Officer either directly or through the applicable privacy mailbox within the division / legal entity, as soon as possible.

When an Information Officer learns of a suspected or actual privacy incident, an internal investigation must be performed, and appropriate remedial measures must be taken in line with the privacy incident management procedures set out in the Group Privacy Framework.

If the investigation confirms that an actual privacy incident has occurred within South Africa, the Information Regulator and impacted Data Subject(s) must be notified in line with the Barloworld privacy incident response plan as set out in the Group Privacy Framework

6.3 Cross-Border Personal Information Flows

The Information Officer of the division / legal entity must determine whether Personal Information may be accessed or transferred across international borders and must approve the transfer prior to it being completed, if not covered under specific Data transfer agreements or other Barloworld policies (serving as Corporate Binding Rules).

Before transferring Personal Information out of South Africa or the country where the Personal Information was collected, adequate safeguards must be in place in line with applicable regulatory requirements, including a determination as to whether the country receiving the Personal Information from South Africa or the country where the Personal Information was collected has privacy / Data

protection laws equivalent to those of POPIA or those of the country where the Personal Information was collected, in consultation with the relevant Information Officer.

A Data transfer agreement will usually be concluded between the legal entity and legal entities outside South Africa or the country where the Personal Information was collected to which the Personal Information will be transferred.

Where Personal Information is transferred out of South Africa, the cross-border transfer decision-making tree set out in the Group Privacy Framework must be used for purposes of decision-making.

6.4 Third Party Risk Management

Before Personal Information is Processed by an external third party on behalf of Barloworld, a legally binding contract must be concluded between Barloworld and the third party that clearly defines the roles and accountabilities for the intended Processing of Personal Information by the third-party.

All third parties Processing Personal Information on behalf of Barloworld must provide adequate assurance of security measures to safeguard the Personal Information being Processed for Barloworld, for which Barloworld ultimately remains accountable.

Barloworld must contractually require the third party to provide the same level of Personal Information protection as Barloworld applies, as a minimum.

The third party must only process Personal Information for purposes of executing its contractual obligations towards Barloworld.

Barloworld must take reasonable measures to ensure that third parties comply with the security requirements specified in the legally binding contract, which must contain the standard privacy and Data protection clauses.

Upon completion / expiration of the contract with the third party, Barloworld must ensure that all Personal Information Processed by the third party is either destroyed or returned to Barloworld in the prescribed manner.

6.5 Data Subject Rights and Notifications

Barloworld is responsible to provide all Data Subjects with a mechanism to access their Personal Information and must have systems and processes in place to enable all Data Subjects to update, rectify, erase, or transmit their Personal Information, for purposes of accuracy and transparency.

A Data Subject rights request procedure has been defined in Group Privacy Framework to address all Data Subject requests and/or complaints in a standard and consistent manner.

If an Employee becomes aware of a Data Subject request, this must be reported directly to the applicable Information Officer or by using the designated privacy mailbox in the division / legal entity.

An external privacy notice (also referred to as a “privacy statement”) must be maintained on all Barloworld websites to inform Data Subjects of how their Personal Information will be Processed.

Relevant notifications must be sent to, or consent must be requested from Data Subjects at the point of collection of their Personal Information. Where changes are made to internal or external privacy statements, notices or policies, Data Subjects must be notified of these changes.

6.6 Processing of Employee Personal Information

A detailed internal privacy statement detailing when and how Employee Personal Information will be Processed for purposes of giving effect to the conditions of employment, will be published on local divisional / legal entity intranets and applicable human capital systems, and will be incorporated by reference in employment contracts.

6.7 Use, Storage, Retention and Disposal of Personal Information

Processes must be implemented to ensure that the purposes, methods, storage limitation and retention period of Personal Information are consistent.

All Personal Information must be adequately protected based on applicable laws, regulations, and recognized industry standards – e.g., POPIA, ISO 27000, ISO 27701, etc.

Suitable measures to prevent and detect unauthorised entry / access to premises where Personal Information may be stored or Processed must be adopted.

Suitable measures to protect IT systems and networks used for Processing Personal Information from unauthorised access, modification and disclosure must be implemented.

Adequate security mechanisms designed to protect Personal Information must be used to prevent such Personal Information from being stolen, misused, or abused, and prevent Information security breaches.

Where Personal Information is stored in printed format, all documents / printed Records must be shredded / disposed of in line with the prescribed retention periods as set out in the Barloworld Group Information and Records Retention and Destruction Policy.

Where Personal Information is stored in electronic / machine-readable format, all storage media must be de-identified, physically destroyed or 'wiped' (over-written with random Information for a minimum of three times) as part of the disposal process when Barloworld is no longer authorised to have such Personal Information.

Devices used to store Personal Information must always either be destroyed or 'wiped' (as above) as part of the Personal Information disposal process when Barloworld is no longer authorised to have such Personal Information.

The manner and technical means of any erasures / deletions must be agreed between the Information Officers, the Group Chief Information Security Officer, and the Chief Data Officer.

Functional Data owners / custodians must be aware of all locations where Personal Information is stored in their environment.

A Records retention working group must be established to provide guidance on the standardization of retention periods within various functions, and across the Group, based on prescribed regulatory requirements or internal risk mitigation requirements.

6.8 Maintaining Personal Information Inventories

The Processing of Personal Information must be documented by each Barloworld division / legal entity within their Personal Information inventories.

The Personal Information inventories must contain, among other prescribed Personal Information, a description of business process categories of Data Subjects and the types of Personal Information, the purposes of the Processing, the legal basis for each Processing activity per business process and details regarding any transfer of Personal Information to third parties and across international borders.

The Personal Information inventories must be reviewed and updated annually, and in accordance with the criteria identified in the Personal Information inventory, to remain up to date.

The Information Officer / deputy Information Officer must have access to the Personal Information inventories and must coordinate the maintenance thereof with the various cross-functional Data owners / custodians as identified in the division / legal entity.

Information Officers must provide periodic reports to the Group Privacy Steering Committee on any material updates made to the Personal Information inventories.

6.9 Prior Authorisation

Barloworld divisions / legal entities operating from South Africa must obtain prior authorisation from the Information Regulator on a once-off basis prior to any Processing, if they plan to[1]:

a) process any unique identifiers (defined as “any identifier that is assigned to a Data Subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that Data Subject in relation to that responsible party”) of Data Subjects for a purpose other than the one for which the identifier was specifically intended at collection; and with the aim of linking the Information together with Information processed by other responsible parties;

b) process Information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties;

c) process Information for the purposes of credit reporting (such as a credit bureau); or

d) transfer Special Personal Information or the Personal Information of children under 18 (eighteen), to a third party in a foreign country that does not provide an adequate level of protection for the processing of Personal Information.

The procedures to apply for such prior authorisation are set out at https://www.justice.gov.za/inforeg/docs/InfoRegSA-Invite-PriorAuthorisation-20210311.pdf.

6.10 Direct Marketing

Privacy laws apply to the collection and Processing of Personal Information for the purpose of managing customer relationships based on the supply of goods and services. It also applies to direct marketing activities, i.e., marketing communication directed to selected / targeted recipients, e.g., by means of various channels, including electronic communication such as emails or SMS, WhatsApp / Messaging applications.

In addition to privacy laws, direct marketing activities are subject to marketing / advertising legislation, which may vary across countries, and may include requirements to obtain consent prior to sending electronic marketing material, or to include the source from which the Data Subject’s contact details were acquired as part of the electronic communication.

The following criteria must be adhered to when Processing Personal Information for direct marketing purposes:

- prior to contacting a customer or potential customer, determine if the customer has formally provided consent for marketing communication and if “opted-in” or has “opted-out” of direct marketing or cold-calling initiatives from Barloworld;
- prior to acquiring Personal Information from a third party (such as lists of contact details acquired from vendors, agents / intermediaries), the third party supplying the contact details must confirm that it has obtained the Personal Information lawfully and has the right to provide such information to Barloworld for marketing purposes;
- Data Subjects must be informed of the use of cookies within privacy statements and by means of a cookie banner prior to placing a cookie on the Data Subject’s device to collect Data; and
- when using Personal Information collected by means of cookies, ensure that the Information is used only in accordance with the Barloworld (external) privacy statement.

The following practices must be avoided when Processing Personal Information on Barloworld systems:

- Processing large amounts of, or categories of, Personal Information which goes beyond what is necessary for managing an existing customer relationship or for pursuing a potential customer. Limit the Personal Information with respect to potential customers to contact details and business-related Data (e.g., business email addresses, business landline, etc.);
- Processing Personal Information obtained from publicly available sources which are not published for marketing purposes, e.g., Information from public Facebook profiles, discussion forums, etc.; and/or
- Processing Data around political opinions, religious beliefs, health or sex life/sexual orientation or other Special Personal Information or Information of children under 18, without the prior consent of the Data Subject, parent or guardian in respect of a child, unless required by Law.

6.11 Privacy Risk Assessments

Privacy risk assessments must be formally performed during the inception of projects that will include the Processing of Personal Information as a core output. This ensures that relevant privacy / Data protection risks are identified and managed sooner rather than at later critical stages of implementation. Privacy risk assessments must be triggered by approval of new projects, systems or business processes resulting in material changes to, or new purposes for the Processing of Personal Information.

All documentation related to privacy risk assessments must be maintained for audit purposes and to facilitate consistent management / review procedures for the continuous improvement of privacy controls.

Upon discovery or realisation of a potential risk to fair and lawful Personal Information Processing practices or Data / security breaches of any controlled Personal Information (or perceived risks to Personal Information), these must be reported to the relevant Information Officer for further management actions.

6.12 Privacy Training and Awareness

All Employees and, specifically the appointed Information Officers and Deputy Information Officers, must be aware of the requirements set out in this Policy as well as their responsibilities regarding the

lawful Processing of Personal Information. • Privacy related training that informs Employees about Barloworld privacy and Information security policies, procedures, processes and systems, and how their specific roles interface with privacy requirements, must be part of Employee onboarding processes and regular privacy training programmes.

All Employees must complete mandatory privacy training modules, which may be role-specific, within a defined periodic training cycle, which must be tracked and reported to the Group Privacy Steering Committee.

Training and awareness initiatives must be reviewed on a regular basis to ensure relevance to current business systems and processes.

6.13 Automated Decision-Making

As a general rule, a Data Subject may not be subject to a decision by Barloworld which results in legal consequences for him, her or it, or which affects him, her or it to a substantial degree, which is based solely on the basis of the automated Processing of Personal Information intended to provide a profile of such person including his or her performance at work, or his, her or its credit worthiness, reliability, location, health, personal preferences or conduct.

The provisions above do not apply if the decision:

- has been taken in connection with the conclusion or execution of a contract, and the request of the Data Subject in terms of the contract has been met; or
- appropriate measures have been taken to protect the Data Subject's legitimate interests; or
- is governed by a law or code of conduct in which appropriate measures are specified for protecting the legitimate interests of Data subjects, which must-
    - provide an opportunity for a Data Subject to make representations about the automated decision; and
    - require Barloworld to provide the Data Subject with sufficient information about the underlying logic of the automated processing of the Information relating to him or her to enable him or her to make such representations.

6.14 Dealing with the Information Regulator

All correspondences, notifications, and communications with the Information Regulator (or equivalent statutory body outside South Africa) must be done by the divisional / legal entity Information Officer or Deputy Information Officers in consultation with the Group Information Officer.

Only the Information Officer or deputy Information Officer must deal with complaints from the Information Regulator. All complaints must be referred to the Information Officer or deputy Information Officer of a division / legal entity.

7 Communication

This policy should be communicated to all Barloworld Employees, Information Officers, deputy Information Officers and Employees whose core job outputs involve the Processing of Personal Information.

8 Related Policies and Other Documents

Document Name
Barloworld Worldwide Code of Conduct
Barloworld Group Privacy Framework
Information and Record Retention and Destruction Policy
Barloworld Group Data Management Strategy

9 Raising Concerns and Seeking Guidance

If any person becomes aware of a circumstance or action that violates or appears to violate this policy on bribery and corruption, they are encouraged to contact their manager, the Group General Counsel, the Group Compliance Manager, or alternatively the Barloworld Ethics Line at www.tip-offs.com.

The Barloworld Ethics Line is an independent and confidential system for reporting allegations of unethical behaviour, illegal actions, or actions that violate the Barloworld Worldwide Code of Conduct.

The Barloworld Global Whistleblowing Policy applies to the use of the Barloworld Ethics Line, and it contains the contact details pertaining to each company, division, or business unit.
Barloworld is committed to ensuring that no employee suffers any occupational detriment as a result of reporting a genuine concern in good faith.

10 Breach of Policy

It is the responsibility of Employees to comply with this Policy and failure to do so could amount to regulatory fines / penalties, third party claims, reputational damage to Barloworld and a material breach of the Employee contract of employment, which may result in a corrective conduct review in accordance with the Group Corrective Conduct Policy, and / or applicable divisional policies / procedures relating to corrective / disciplinary actions.

11 Deviations from Policy

It is the responsibility of divisional executive management to ensure that this Policy is adopted and approved by an appropriate divisional executive committee.

Any deviations to this Policy that amend the meaning or lower the minimum standard of the Group policy requirements must be pre-approved, in writing by Group Information Officer. Once approved, such deviations must be tabled, approved and recorded at an appropriate Group and divisional executive meeting. Any deviations that add more specific requirements, and therefore higher the minimum standard required by this Policy, may be included at the discretion of divisional executive management and then tabled, approved and recorded at an appropriate divisional executive meeting.

Any deviations that add more specific requirements, and therefore lower the minimum standard required by this Barloworld policy, may be included at the discretion of executive management and then tabled, approved and recorded at an appropriate executive meeting.

Language translations of Barloworld policies must be conducted or checked by a professional language translator to avoid translation errors that may change the meaning of the policy requirements.