Group Data Privacy Framework

Classification	INTERNAL		
Document Type	Framework		
Policy Reference Number	BW-GRP-LEG-005		
Area of Applicability	Barloworld Group		
Policy Owner	Group General Counsel		
Policy Owner Contact Information	Email: Sandile.Langa@barloworld.com Tel: 011 445 1010		
Version	V1.0		
Date Approved	TBC		
Approved by	Risk Committee		
Policy Sponsor	Group Finance Director		
Effective Date	TBC		
Next Review Date	January 2025		
Documentation Status	☐ Working draft	☐ Consultation Release	☐ Final version

APPROVAL AND OWNERSHIP

Policy Owner	Date
Group General Counsel	January 2023

Approved By	Date
Risk Committee	TBC
Executive Committee	TBC

REVISION HISTORY

Version	Revision Date	Description	Next review Date
V1.0		New Document	January 2025

Contents

DEFINITIONS AND ABBREVIATIONS

Table 1: Definitions

Terminology	Description

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
POPIA	Protection of Personal Information Act
GDPR	European Union’s General Data Protection Regulation
PAIA	Promotion of Access to Information Act
PRA	Privacy Risk Assessment

1 Preamble and Summary

Barloworld Group (“Barloworld”) recognises information protection as a business imperative first and foremost, and secondly as a regulatory, legal and reputational issue. The evolving global Privacy regulatory landscape encourages the need for organisations such as Barloworld to strives to comply with applicable information protection laws and regulations related to Information Privacy ("Privacy") in countries where it operates.

In South Africa, the Protection of Personal Information Act ("POPIA") exists as the country's first piece of comprehensive data protection legislation. POPIA aims to protect the Personal Information of individuals and juristic persons by regulating how organisations such as Barloworld process the Personal Information of individuals and juristic persons. Further, POPIA seeks to promote transparency concerning the collection and processing of Personal Information.

Due to the nature of operations in Barloworld, Privacy compliance practices are aligned with the local Privacy laws as well other globally recognised and leading laws and regulations such as the European Union's General Data Protection Regulation ("GDPR").

Barloworld's reputation relies on a culture of integrity and accountability that is reflected in the behaviours of our people and our suppliers involved in the processing of Personal Information on behalf of Barloworld. Therefore, Barloworld has zero tolerance for deliberate misconduct that undermines this standard. Instances of unintended ethical failures as it relates to the processing of Personal Information will be addressed on a prioritised basis.

2 Purpose and Objective

Based on the nature of operations in Barloworld, Personal Information of natural and juristic persons is processed to promote and facilitate business transactions. Barloworld processes Personal Information of its employees, third party vendors, clients and other key stakeholders such as investors and shareholders.

In processing Personal Information as listed above, there are risks associated, which include but are not limited to loss, theft, unauthorised access, or accidental disclosure. These can lead to detrimental consequences such as fines, reputational damages, and sanctions. The protection of Personal Information to reduce the likelihood of these risks is of paramount importance.

The purpose of this Privacy Framework is to establish a blueprint for Barloworld in regard to Privacy Compliance in alignment with the Barloworld Group Privacy Policy. The Privacy Framework constitutes Barloworld's Privacy Governance and Privacy operating model highlighting Barloworld's roles, structure and operating capabilities to ensure oversight, alignment and consistency to Barloworld's understanding of Privacy threats and risks as well as management of these across Barloworld's policies, people, business processes and technology. As such, the Privacy Framework will promote Privacy compliance in line with the relevant Privacy legislation, thus improving Barloworld's Privacy compliance posture and overall culture.

3 Scope

The requirements contained in this framework apply to Barloworld and its subsidiary companies or divisions and all employees (temporary and/or permanent), contractors, service providers and consultants, or any other person assigned with specific duties of processing Personal Information on behalf of Barloworld.

4 Privacy Compliance Drivers

Barloworld adheres to global privacy standards and best practices and has based its Privacy Compliance Drivers from the conditions for lawful processing of Personal Information as set out in Chapter 3 of POPIA ("Processing Conditions"). These Privacy Principles (set out in Figure 1 below) are to ensure that the processing of Personal Information in Barloworld is of a lawful nature.

Privacy Principles for the lawful processing of Personal Information

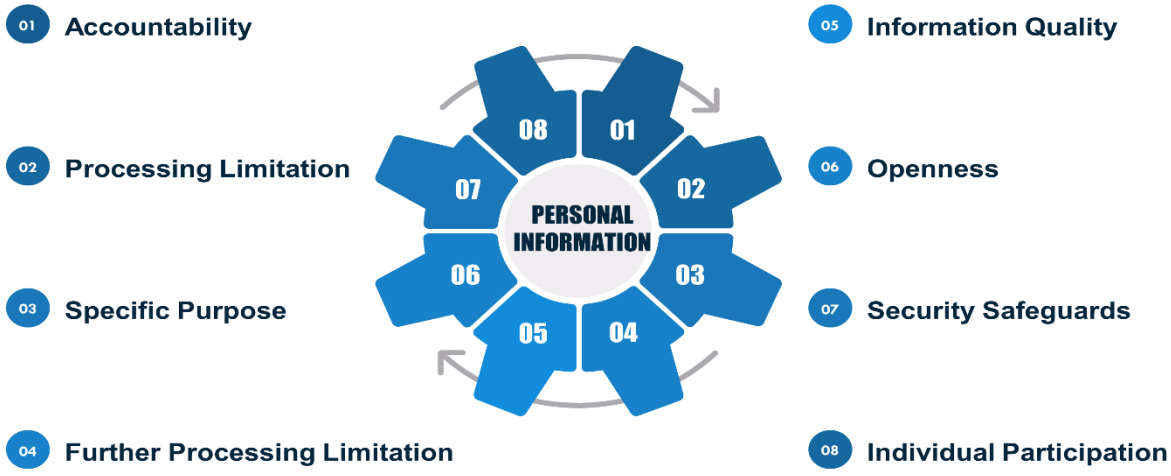

Figure 1 Privacy Principles

1 - Accountability

Barloworld must ensure compliance with relevant data privacy legislation.

2 - Processing Limitation

Personal Information must be processed lawfully with the consent of the data subject.

3 – Purpose Specification

Personal Information must be collected for a specific and lawful purpose.

4 - Further Processing Limitation

Barloworld may only process the information for the purpose it was originally collected.

5 - Information Quality

The Personal Information must be complete and accurate.

6 - Openness

Notification must be provided to the data subject of the processing of their Personal Information.

7 - Security Safeguards

Security measures must be in place to prevent loss, damage or theft of Personal Information.

8 - Individual / Data Subject Participation

Barloworld must be able to provide a data subject access to their Personal Information if required.

5 Barloworld Data Privacy Compliance Framework

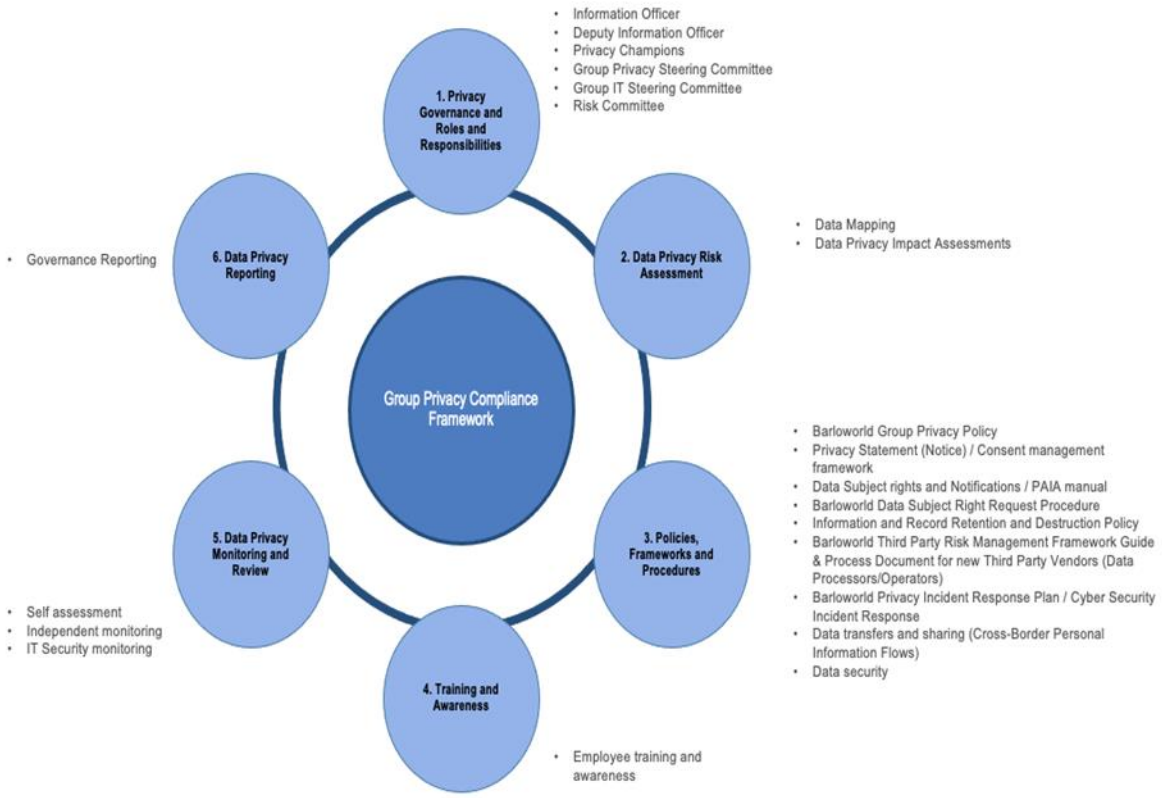

Figure 2 Data Privacy Compliance Framework

A. Data Privacy Compliance Framework Sections:

5.1 Privacy Governance and Roles and Responsibilities

5.1.1 Privacy Governance

Privacy Governance outlines the set of accountabilities, roles, responsibilities for Barloworld's stakeholders to support and enable the delivery of the roadmaps and overall Privacy Compliance Programme efforts. Privacy Governance includes the development and enforcement of various Privacy Policies and Procedures implemented to ensure compliance with Data Privacy laws and regulations. Please refer to section 5.3. for the detail on the various Policies and Procedure implemented within Barloworld with regard to the processing of Personal Information.

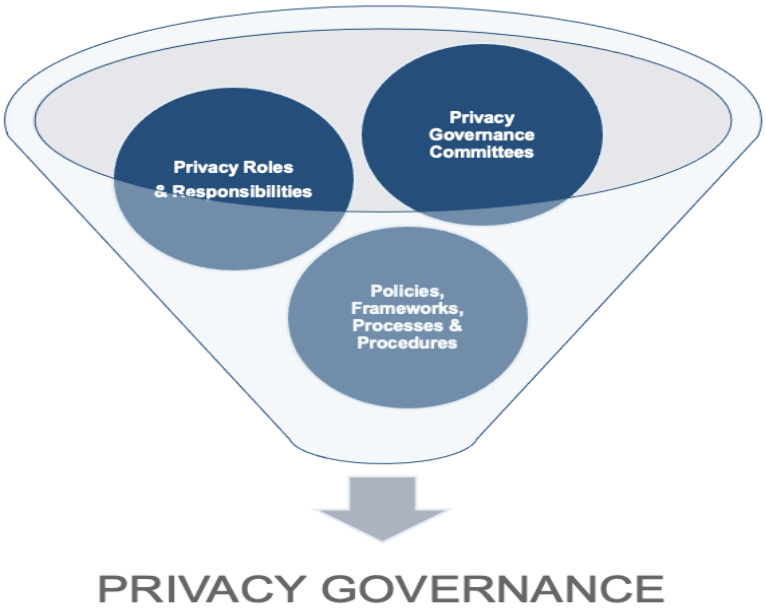

Figure 3 Privacy Governance

5.1.2 Roles and Responsibilities (Accountability)

The diagram below displays at a high level the Barloworld Privacy roles that are in place.

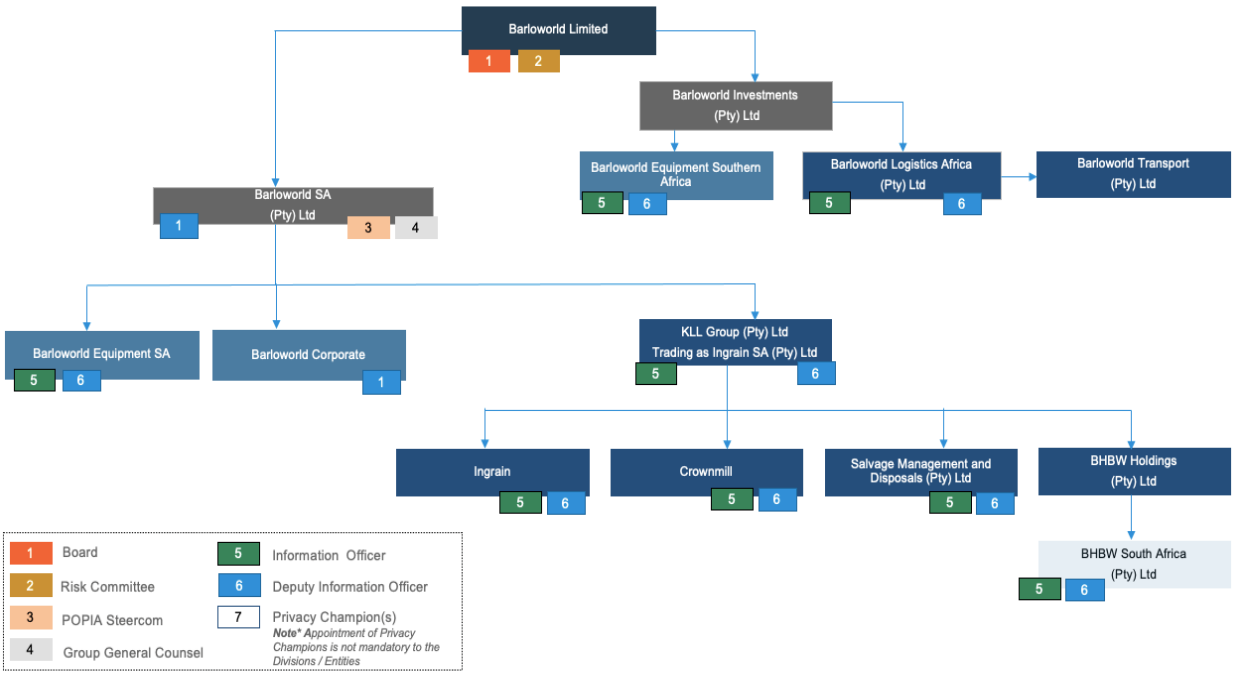

Figure 4 Privacy Roles

Note: Privacy management and authority is not applicable to joint ventures that are noted within the detailed Group structure.*

5.1.2.1 Barloworld Group General Counsel

Over and above the Information Officer responsibilities noted in the section below, the Barloworld Group General Counsel is responsible for:

- Developing and maintaining the Group's Privacy Governance, policies, oversight, and accountability models to identify and track privacy risks/trends and remediation activities as they relate to privacy legislation compliance across the Group.
- Developing and maintain the Group PAIA manual.
- Providing advice, interpretations and guidance regarding privacy legislation and its regulations that applies to the Group.
- Defining the Privacy Framework and to drive implementation of this throughout Barloworld.
- Defining reporting mechanisms to the Information Regulator as it relates to Barloworld.
- Liaising with the Information Regulator, involving the applicable Divisional/Entity Information Officers, regarding privacy matters, complaints, or investigations before the Information Regulator
- Ensuring there Is a the single point of contact for any Privacy matters arising from the Information Regulator as it relates to Barloworld.
- Driving regular Privacy compliance reviews across Barloworld.
- Providing guidance which relates to Personal Information impact assessment ensure that adequate measures and standards exist to comply with the conditions for the lawful processing of Personal Information across Barloworld.
- Reporting and escalating to oversight forums such as the Barloworld committees as outlined in Figure 6 non-compliance, privacy risks and incidents.
- Providing guidance to Barloworld assurance functions enabling them to conduct the required privacy risk assessments and monitoring. In conjunction with these assurance functions, ensure that there is adequate coverage (review, monitoring, testing etc) for information privacy and protection.

5.1.2.2 Information Officer

In line with requirements of Privacy legislation, the Information Officer at each Divisional/Entity level remains ultimately accountable for overseeing compliance with Privacy legislation and regulations, including access to Personal Information. In addition, the Information Officer is responsible for:

- Defining and driving a Privacy Compliance Programme within Barloworld or the respective legal Entity, and delegating responsibility in this regard to the Deputy Information Officers and Privacy Champions in order to implement the programme and drive Privacy compliance.
- Adopting the Privacy Framework and to drive implementation of this throughout respective Divisions / Entities.
- Adopting reporting mechanisms to the Information Regulator as it relates to the respective Division/Entity.
- Liaising with the Information Regulator through the Barloworld Corporate Information Officer in relation to Divisional/Entity specific privacy matters that are before the Information Regulator.

- Ensuring there is the single point of contact for any Privacy matters arising from the Information Regulator.
- Defining and driving the required policies, procedures, standards and guidelines for Divisions, Entities, functions and employees processing Personal Information.
- Ensuring Personal Information impact assessment is done to ensure that adequate measures and standards exist to comply with the conditions for the lawful processing of Personal Information.
- Providing strategic guidance to the relevant committees to ensure compliance with Privacy requirements.
- Defining Privacy training requirements and drive the delivery of such training for all levels of employees within the respective Division /Entity.
- Driving regular Privacy compliance reviews across Divisions / Entities.

The Information Officer in each Divisional/Entity level (with the assistance of the Divisional Deputy Information Officers and Privacy Champions is ultimately accountable to handle and manage Data Subject Right Requests and access to Personal Information requests as per the requirements of the Promotion of Access to Information Act (PAIA).

5.1.2.3 Deputy Information Officer

POPIA states that a Deputy Information Officers should be delegated to at the highest management level. Upon delegation of Privacy compliance responsibilities by the Information Officer, Divisional/Entity level Deputy Information Officers are responsible for:

- Overseeing compliance with Privacy legislation and regulations at Divisional and Entity level.
- Implementation of Privacy Compliance Programmes as defined and overseeing the Division's and Entity's compliance with the Privacy Programme, especially as it pertains to business processes.
- Implementation of, and ongoing monitoring of compliance with, policies, procedures and standards defined for Division's and Entity's functions and employees processing Personal Information (i.e., Personal Information inventories, employment contract clauses, record retention and destruction, data subject rights requests, consent management requirements, investigation of privacy incidents).
- Supporting the Information Officer on Privacy compliance matters through ongoing reporting of Privacy matters to relevant committees.
- Maturing Privacy controls in line with growing business needs.
- Assisting the Information Officer to identify training requirements and the roll-out of training.
- Triggering reviews of Policies by the appropriate Policy owners.
- Performing periodic risk reviews to identify internal and external Privacy risks and derive risk mitigation plans.
- The identification, storage, protection, retrieval and disposal of Personal Information within their respective Divisions and Entities, or functions in line with the Privacy policies, procedures and processes defined.

5.1.2.4 Privacy Champions

Where required, at each Divisional/Entity level, the roles of the Information Officer and Deputy Information Officers are further supported by Privacy Champions. Privacy Champions are mainly for driving the implementation of Privacy controls established as part of Barloworld's Privacy Compliance efforts, as well as ensuring ongoing compliance monitoring. Some of the critical responsibilities of the Privacy Champions' role include:

- Driving implementation of Privacy controls to promote compliance with Privacy legislation and regulations at a business level.
- Supporting the Deputy Information Officer to drive implementation of the Privacy Compliance Programme as defined and to ensure functional compliance with the Privacy Compliance Programme, especially as it pertains to change management (training and awareness), business processes at Divisions and legal Entities.
- Supporting the Deputy Information Officer with the implementation of, and ongoing compliance with, policies, procedures and standards defined for the Division, legal entity and/ or employees processing Personal Information (i.e., Personal Information inventories, employment contract clauses, record retention and destruction, data subject rights requests, consent management requirements, investigation of privacy incidents, identification of cross-border flows and requirements).
- Triggering review of Policies by the appropriate Policy owners in a specific business function.
- Assisting the Deputy Information Officer with the roll-out of privacy training initiatives in a specific business function.
- Identifying Privacy risks and assisting with developing risk mitigation plans at Divisional, Entity and/ or business function level.
- Assisting the Deputy Information Officers and Information Officer with relevant privacy related queries from various data subjects (e.g., employees, customers or other third parties for the Division, Entity or business function).
- Reporting Privacy compliance to Deputy Information Officers and the Information Officer via the established reporting structures.
- Reporting any privacy related incidents, breaches or potential incidents/ breaches that take place Divisional, Entity and business function level and assisting the Information Officer and Deputy Information Officers with related investigations and remediation, where applicable.

Note: The role of the Privacy Champion is more of an operational role that is responsible for the delivery of Privacy compliance at a specific business function for a specific type of data subject (e.g. a Privacy Champion can be an employee in the Human Capital functions responsible for processing employee related Personal Information).*

5.1.2.5 Privacy Reporting Committees

Barloworld has established various committees that govern and manage Barloworld's efforts in relation to privacy and the protection of Personal Information. These committees are embedded at all levels of the business, including the Barloworld Limited Board, Risk Committee level and the Group Privacy Steering Committee Level as depicted in figure below.

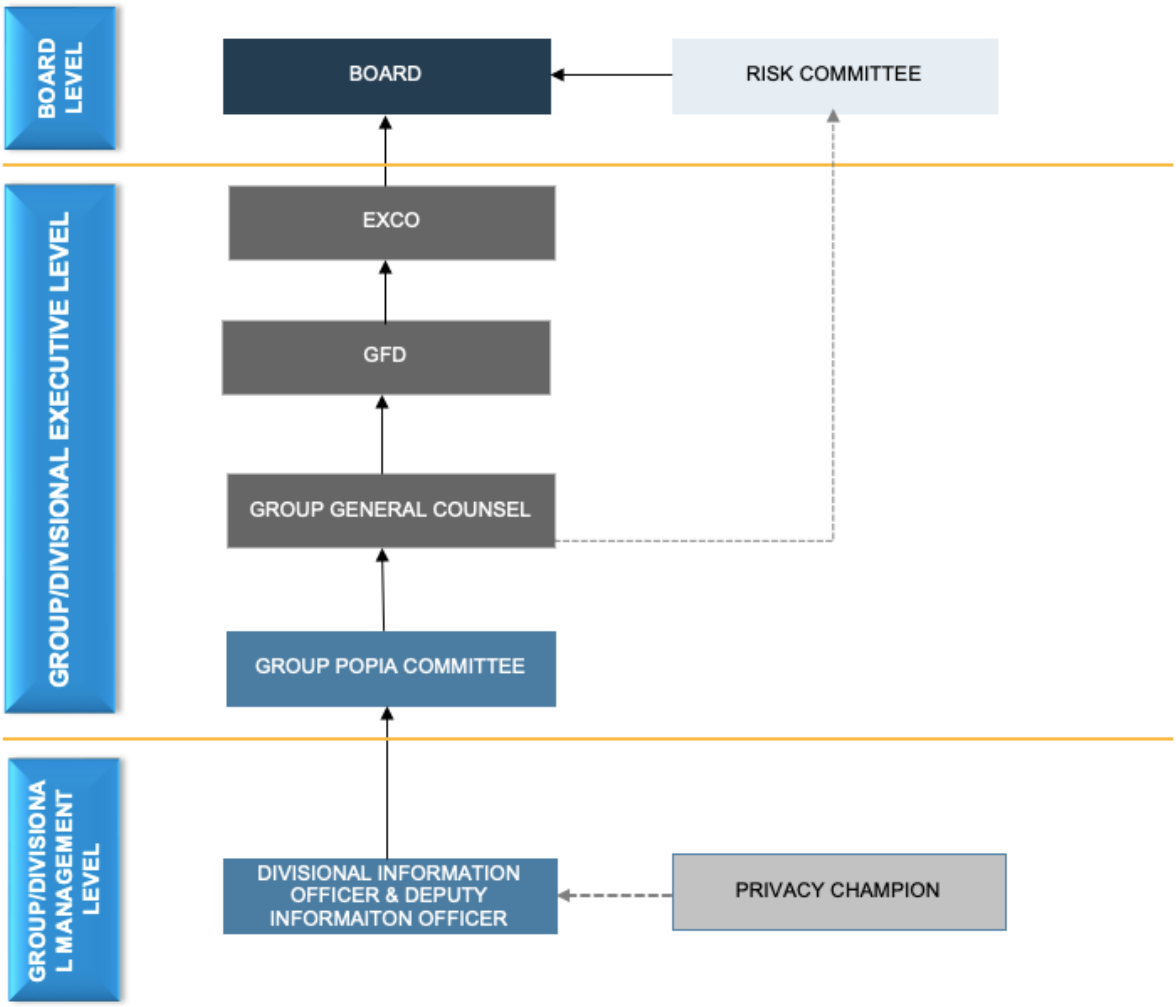

Figure 5 Privacy Reporting Committees

5.1.2.6 Board

The Board of Directors of Barloworld (**Board**) has a duty to ensure that the requisite systems, practices, and culture are in place to manage the privacy risks to which Barloworld is exposed. It is the Board's responsibility to oversee that Barloworld complies with data privacy and protection laws, regulations, and supervisory requirements. It is the Board's accountability to ensure that Barloworld complies with data privacy and protection laws, regulations, and supervisory requirements.

The Board discharges their duties in relation to privacy by delegating their responsibilities to the appointed individuals, committees and functions as set out below.

5.1.2.7 Risk Committee

The Risk Committee in Barloworld is responsible for assisting senior management and/or the Board in reviewing the adequacy and effectiveness of the risk management process, risks faced by the Group and mitigating controls and activities. In this regard, a privacy risk management process, which includes activities such as identification, measurement, evaluation, assessment monitoring and reporting of privacy compliance risks; must be carried out.

5.1.2.8 Group Privacy Steering Committee

The objectives of the Group Privacy Steering Committee include:

- Supporting the Information Officer in ensuring that Privacy controls are implemented in Divisions and Business Units.
- Performing regular reviews and where necessary, recommend actions to increase the effectiveness and impact of the Privacy implementation within Divisions, Entities and Business Units.
- Making critical design decisions with the Information Officer regarding aspects directly impacted by certain business functions (i.e. the development of clauses, updating registration forms, etc.) whilst ensuring that the Privacy Programme's key deliverables are considered and incorporated.
- Performing periodic risk assessments to identify internal and external risks to Personal Information and how these can be mitigated.
- Discussing and making recommendations related to the Privacy remediation and implementation Programme, including objectives, priorities, and matters of significant risk to the Privacy Implementation Programme's success.
- Reporting highlights, risks, issues and decisions made monthly to the other appropriate stakeholders (Divisional Excos, Risk and Sustainability Committee via Internal Assurance and Risk reports).

5.2 Data Privacy Risk Assessment

Data Privacy risk assessment is a process that ensures that data privacy compliance risks are effectively identified, assessed, managed, monitored and reported on. Barloworld's data privacy compliance risk assessment process consists of two phases: Data Mapping and Privacy Risk Assessment.

5.2.1 Data mapping

Data mapping is the process of inventorying the Personal Information in your business systems throughout the lifecycle of the Personal Information. This inventory is called a data map and accurately identify critical elements within the data landscape, including the data types that are collected, how it is collected, their locations, formats, and the processing activities performed on that data including destruction. An up-to-date data map is vital for compliance with modern data privacy regulations.

Barloworld develops and maintains data maps for all its Business Units. These data maps are reviewed on an annual basis to reflect changes in the way Personal Information it collected and processed.

5.2.2 Privacy Risk Assessment

The key objective of a Privacy Risk Assessment ("PRA") is to ensure adequate design of controls in respect of privacy related risks, during the development of new processes or systems as well as when managing the entire contractual relationship with Operators. Barloworld must conduct PRA on all new and existing Barloworld systems, projects and Operator's to ensure their conformity with internal rules and legal/regulatory requirements in relation to privacy and data protection. A PRA seeks to evaluate a proposed project, system or service (or the effects of proposed changes to existing projects, systems or services) from the perspective of the Barloworld Group Privacy Framework, Group Privacy Policy and relevant privacy legislation.

The main aim of a PRA is to identify and reduce future adverse privacy impacts, as well as to inform decision makers as to whether or not to proceed with a project, system or contract with an Operator and on what terms. The PRA ensures that privacy principles as outlined in the Barloworld Privacy Policy are complied with throughout the lifecycle of the intended project, system, process or Operator service.

5.3 Policies, Frameworks and Procedures (Processing, Purpose, Quality, Openness, Security, Data Transfers, Data Security)

To improve the Barloworld's Privacy compliance posture, several policies, processes and procedures have been developed and adopted. These assist with managing Personal Information in line with relevant Privacy legislation. This section, which is subject to change based on Barloworld's Privacy requirements, lists the various policies, frameworks, processes and procedures that form part of Barloworld's Privacy Framework.

5.3.1 Barloworld Group Privacy Policy

The purpose of the Barloworld Group Privacy 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. This Privacy Policy is the first Corporate Binding Rule level and is supported by this Framework which serves as a standard operating model regulating privacy compliance within the Group.

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 the Privacy Policy along with the Group Privacy Framework will apply as Corporate Binding Rules.

5.3.2 Privacy Statement (Notices) / Consent management framework

The purpose of the Barloworld Privacy Statement and the Barloworld Consent Management Framework is to ensure that Barloworld's employees, customers, third party vendors and other key stakeholders, collectively referred to as Data Subjects, are informed about what Personal Information Barloworld collects and processed when engaging with Barloworld and to maintain a framework for managing consent received from these Data Subjects throughout the end-to-end Personal Information life cycle and it outlines how consent is managed.

5.3.3 Data Subject rights / PAIA manual

The Barloworld PAIA Manual is intended to ensure that Barloworld complies with POPIA and to foster a culture of transparency and accountability within Barloworld by giving effect to the right to information that is required for the exercise or protection of any right and to actively promote a society in which Barloworld's Data Subjects have effective access to their Personal Information to enable them to exercise and protect their rights.

5.3.4 Barloworld Data Subject Right Request Procedure

The Barloworld Data Subject Request Procedure defines the procedure for the handling of requests made by Data Subjects regarding their Personal Information held by Barloworld.

These rights include access to, confirmation, correction, export and deletion of information, including Personal and Sensitive Personal Information held by Barloworld. The Data Subject Rights Request Process and Procedure aim to:

- Document the procedure for managing Data Subject Right Request processes within Barloworld.
- Ensure roles and responsibilities are clearly articulated and communicated for the stakeholders involved in this Process and Procedure.
- Ensure consistent methods of response to Data Subjects who have exercised their applicable Privacy rights; and
- Ensure regulatory requirements are met.

5.3.5 Information and Record Retention and Destruction Policy

The Barloworld Information and Record Retention and Destruction Policy provides Divisions/legal Entities with

minimum standards and guidelines on the retention, archival and destruction of business information and records.

5.3.6 Barloworld Third Party Risk Management Framework Guide & Process Document for New Third Party Vendors (Data Processors/Operators)

Barloworld recognises the risk associated with Third Party Vendors (TP) and as such have developed a Framework to profile and assess the Privacy risk exposure that TPs pose to Barloworld. The Framework consists of two key assessments, namely the:

- Privacy Risk Profiling Assessment that constitutes of a profiling questionnaire and risk rating criteria to determine the inherent Privacy risk of a third party; and
- Privacy Due diligence Assessment that constitutes of a due diligence questionnaire and risk rating criteria to determine the residual Privacy risk of a third party.

Privacy Risk Profiling determines the inherent Privacy risk that a TP poses to Barloworld based on a set of criteria. The criteria will be included as part of a Tender when the scope has been defined and agreed to include Privacy as a key scoping item (i.e., the services required will impact the processing of Barloworld Personal Information).

5.3.7 Barloworld Privacy Incident Response Plan / Cyber Security Incident Response

The Barloworld Privacy Incident Response Plan and the Cyber Security Incident Response Plan has been developed to provide direction and focus on the handling of privacy and information security incidents that adversely affect the Barloworld group of companies.

The purpose of these plans is to equip the Group to respond quickly and appropriately to privacy and information security incidents.

5.3.8 Data transfers and sharing (Cross-Border Personal Information Flows)

During its activities the Barloworld Group will collect, store and process Personal Information about the Barloworld Group's staff, customers, suppliers and other third parties. Such information may be transferred across various jurisdictions. The following measure are in place to ensure the protection of Personal Information during the transfer and or sharing stages of the information Lifecyle:

- **Data Transfer Agreement**: The Data Transfer Agreement is measure in which Barloworld, as an information exporter, aims to ensure that the protection of Personal Information belonging to its Data Subjects is maintained by the relevant information importer. Information Officers must ensure that the Data Transfer Agreement is in place prior to any transfer of Personal Information, including cross-border transfers.
- **Binding Corporate Rules and Privacy Policy**: In instances where Barloworld legal Entities share Personal Information for a defined lawful basis, unless stated by law, sharing of such information must be done in compliance with the Barloworld Binding Corporate Rules and Privacy Policy.

5.3.9 Data security

Information and Cyber Security division must maintain the security safeguards necessary to prevent unauthorised access to, or unauthorised disclosure of Personal Information. All Personal Information must be adequately protected based on applicable laws, regulations, and recognized industry standards – e.g., POPIA, ISO 27000, ISO 27701, etc.

In addition, Information and Cyber Security division is responsible for the development, maintenance and implementation of the Group information and cyber security and cyber incident management policies and standards.

5.4 Training and Communication

Training and communication programs are vital to ensure the establishment and maintenance of a Barloworld Data Privacy compliance culture. It also ensures that all employees and/or stakeholders understand the boundaries within which the business divisions must operate. Training and communication are one of the most important lines of defence for a regulatory compliance program.

5.4.1 Training

Training provides the knowledge and skills needed to employ the organisation's policies and procedures, and deal with any potential Data Privacy non-compliance problems or issues that may arise.

Guidance on Data Privacy Training:

- Training should be proportionate to the level of risk and role based;
- General awareness training should be completed by all employees in a 2-year cycle;
- Induction training for new employees covering all Data Privacy policies;
- Ad-hoc training sessions on a specific Data Privacy topic or policy;
- Training can take both face-to-face and e-learning format;
- Training records and attendance must recorded be preserved; and
- Training content should be bi-lingual where the official state language is not English.

5.4.2 Communication

To continuously enhance and maintain the Barloworld's Data Privacy compliance culture, the Regulatory Compliance Function must drive Data Privacy compliance awareness through:

- involvement in the New Employee Orientation Programme (Induction training);
- contributions to business publications, on a quarterly basis;
- communicating its RC standards via the Supplier Code of Conduct which needs to be signed by all third-party service providers and suppliers; and
- awareness campaigns.

5.5 Data Privacy Monitoring and Review

It is the accountability of the Divisional/Entity Information Officers, Deputy Information Officer, and the Privacy Champions to ensure continuous oversight, monitoring and compliance with the Group Data Privacy

requirements. They must develop an annual monitoring plan for the monitoring of implemented Data Privacy controls, indicating the frequency of monitoring that will be undertaken as well as the various areas that will be monitored. The purpose of conducting regulatory compliance monitoring and reviews is to:

- identify and improve areas of regulatory compliance weaknesses;
- ensure controls are properly implemented and working effectively;
- ensure that follow up action plans are drafted, considered, and implemented by management where non-compliances have been identified or controls are found to be ineffective.

Monitoring must be conducted as set out in the Barloworld Regulatory Compliance Framework.

5.6 Data Privacy Reporting

The status of privacy compliance must be reported to the various governance committees at Divisional/ legal Entity and Barloworld Group level. Monthly/quarterly and ad hoc reports may be required when deemed appropriate.

5.6.1 Divisional level Reporting

The Divisional Privacy Champions must report the status of privacy compliance to Divisional management and relevant governance committees (Privacy Steering Committee) quarterly. The report must include the Division's / legal Entity's past privacy compliance events (such as Data Subject rights requests), privacy compliance process updates and progress, awareness training conducted and planned initiatives, privacy compliance areas of concern or high risk and privacy non-compliances.

5.6.2 Group

The Divisional/Entity Information Officers must report the status of privacy compliance to EXCO and relevant governance committees quarterly. The report must include the past privacy compliance events (such as Data Subject rights requests), privacy compliance process updates and progress, awareness training conducted and planned initiatives, privacy compliance areas of concern or high risk and privacy non-compliances.

5.6.3 Regulatory Reporting and Filings (as applicable by law)

The Barloworld Corporate Information Officer with involvement from the applicable Divisional/Entity level Information Officer(s) is responsible for maintaining a relationship with the Information Regulator and providing the required reporting mechanisms where appropriate. This includes reporting for any applicable regulatory filings upon a defined period.

6 Regulatory Background

Barloworld adheres to global privacy standards and best practices and has based this framework 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.

7 Related Policies and Other Documents

Document Name
Group Privacy Policy
Barloworld Privacy Awareness Employee Handbook

8 Raising Concerns and Seeking Guidance

If any person becomes aware of a circumstance or action that violates or appears to violate this framework 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.

9 Breach of Framework

Compliance with the Framework is the responsibility of all Barloworld employees including Policy Owners and Stakeholders and failure to do so could amount to misconduct and a material breach of the contract of employment.

10 Deviations from Framework

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

Any deviations to this framework that amend the meaning or lower the minimum standard of the framework 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.

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