Privacy Policy

29 June 2021

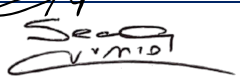
Table of contents

1 Document Administration

1.1 Revision History

Version	Date	Author	Description of change
1.0	2020/10/14	CISO Imperial	Draft
2.0	2021/06/29	M Kerrigan	Revision to Pple

1.2 Approval List

Name	Designation	Date	Signature
Phillip Meyer	Chief Executive Officer	01/07/2021	
Sean Permuy	Chief Commercial Officer	01/07/2021	

1.3 Definitions / Acronyms

Abbreviation	Description
CISO	Chief Information Security Officer
Data / Information asset	Information, in either electronic or paper form, that has value because its use is necessary for the execution of operations and the achievement of goals for Pple .
Data / Information asset owner: Business Head	The operating company head charged with accountability for the management of the information asset in order to attain the business objective, while satisfying the demands of legislation and information management best practice.
Data / Information processing	Any operation or activity or any set of operations, whether or not by automatic means, including a) the collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation or use; b) dissemination by means of transmission, distribution or making available through any other form; or c) merging, linking, as well as restriction, degradation, erasure, pseudonymizing or destruction of information.
Data / Information processing facilities	Any device, equipment, service, system, hardware, software or network that is used to process the Pple owned information in either electronic or paper form, or any physical location that houses any of the aforementioned.
Data Protection Officer (DPO)	The individual(s) accountable with satisfying the requirements of the General Data Protection Regulation (GDPR)
Data Subject / Data owner	Refers to the individual to whom the Personal Data / Information relates, could be internal or external.
Encryption	Methods used to convert or re-organise data or information into a form that hides the original content of the data or information.

Abbreviation	Description
Functional unit	Any Pple functional unit, business unit or supporting function.
Functional head	The leader of a Pple functional unit, business unit or supporting function.
General Data Protection Regulation (GDPR)	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 The primary legislation governing Privacy in the European Union
ICT	Information and Communications Technology
Information Asset Owner or creator (Data Owner): Business Owner	The party with the authority to determine who may create, access, modify or delete information. This is usually a business, not IT function.
Information Officer	The individual accountable with satisfying the requirements of PoPIA
Intercept	The acquisition of the contents of any communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication, and includes the: • Monitoring of any such communication by means of a monitoring device; • Viewing, examination or inspection of the contents of any indirect communication; and • Diversion of any indirect communication from its intended destination to any other destination. Note that this will include activities such as the viewing of static mails or files residing on servers.
Juristic Body	As opposed to a Natural Person, a Juristic Body is a non-living entity regarded by law to have the status of personhood. In the context of this policy: Companies, Partnerships, Corporations, Limited Liability Companies, Non-Profit and Tax-Exempt Corporations, Sole

Abbreviation	Description
	Proprietorships, Governmental and Semi-Governmental Organizations.
Legal Person	Any entity (Natural Person or Juristic Body) that can do the things an everyday person can usually do in law - such as enter into contracts, etc.
Logical access	The process of being identified, authenticated and authorized in order to use IT systems.
Natural Person	An individual human being, as opposed to a Legal Person. In the context of this policy: staff, contractors, customers and all persons engaging with Pple .
Need-to-know principle	A principle that states that individuals should only be granted access to information if they require that information to carry out their duties or any tasks assigned to them.
Personal Data / Information	Information relating to an identifiable, living, natural person, and where applicable and identifiable, existing juristic person[1], including but not limited to a) information relating to 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, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person

[1] Note that not all privacy legislation or regulations include Juristic Bodies (companies) in the definition of personal data / information. For purposes of this policy, in the interests of creating a common set of principles, and as it does not significantly change the operating procedures Juristic Bodies are included in the ambit of this policy.

Abbreviation	Description
	d) the biometric information of the person, including identifiable video imagery of a person, and fingerprint data retained for access control purposes 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 h) 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 i) information relating to call data records which is a data record produced by telecommunications equipment that documents the details of a telephone call or other telecommunications transaction that passes through the mobile network. j) From GDPR: Genetic data, defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.
PoPIA	Protection of Personal Information Act, 4 of 2013; the primary legislation governing Privacy in South Africa
Special Personal Information	Special personal information includes information concerning a child and personal information concerning the religious or philosophical beliefs, race or ethnic origin, trade union membership, political opinions, health, DNA, sexual life or criminal behaviour of a data subject. Special Personal Information is generally treated more stringently in law than Personal Data / Information.

Abbreviation	Description
System Owner(s)	The party responsible for defining the business requirement to be addressed through a system implementation, budgeting for the acquisition and deriving business value from the system operation.
User	User refers to any individual, whether employee, contractor or third party, that makes use of Pple information systems or information assets. This includes connecting to Pple information systems remotely.

2 Overview

2.1 Purpose

The aim of this Policy is to

- ensure compliance to the relevant privacy legislation/regulations across the different jurisdictions of the Pple 's (hereafter referred to as Pple) operations;
- educate the business on why the adherence to privacy legislation/regulation is important and the potential consequences of failing to comply; and
- inform the business of the procedures in place for dealing with any breaches that affect Pple Stakeholders.

2.2 Scope

This Policy is applicable to the following:

- All personal data / information including but not limited to customer information, Pple employees, third party and Pple company related information generated, processed and stored by operating companies at Pple to perform its activities and delivery of services;
- All systems and processes used in the course of managing personal data / information;
- Unless stated otherwise, this policy applies to all employees, contractors and third-party personnel of Pple and operating companies accessing Imperial information processing facilities. Pple information processing facilities include, but not limited to; Pple facilities, offices, work areas, secure areas, critical

infrastructure rooms (CIR), telecommunications rooms, warehouses and depots as well as solutions that may be used in road-, water- and air-borne vehicles.

2.3 Audience

This policy applies to all individuals authorized to access Pple information processing facilities. This Policy is also applicable to the information that is handled and processed by contractors and third parties for Pple and any Operating Companies.

2.4 Non-Compliance

Non-compliance with this policy must be reported to the Pple Information Officer. Any breach may result in disciplinary action being taken, which may include dismissal.

Any disciplinary action arising from breach of this document will be taken according to the disciplinary code and grievance procedure of Pple . Where an employee is suspected of breaching the document, an internal investigation will be undertaken, depending on the outcome, civil and/or criminal legal action could be taken against the employee.

2.5 Associated Policies

Reference	Policy
IP-IC	Information Classification Policy
IS-IH	Information Handling Standard
IS-IL	Information Labelling Standard

3 Policy Statements

3.1 Introduction

This policy addresses the requirements of legislation across different domains. As the legislation uses different terminology, for purposes of this policy the terms "Personal Data" and "Personal Information" have the same meaning and are used interchangeably.

Pple takes the Privacy of Sensitive and Personal Information of all its stakeholders seriously. Pple understands that sensitive and personal information is important to all stakeholders and is committed to protecting stakeholder privacy. Pple 's Privacy Policy incorporates relevant legislation as a guideline for sensitive or personal:

- Data Collection;
- Data Retention and Security;
- Data Usage and Disclosure;
- Data Accessibility;
- Data Correction; and
- Data Breach procedures.

3.2 Information Collected by Pple

Pple generally collects some or all of the following sensitive/personal information about individual stakeholders when they gain employment or provide information for business purposes:

- Name including any use of a pseudonym;
- Address, phone details and email contact details;
- Employment history;
- Bank account details;
- National identifiers;
- Referee opinions;
- Interview opinions; and
- Any other information that is supplied on documentation or in communications with an Pple representative.

3.3 How Pple Obtains Data

Pple obtains most personal information directly from an individual stakeholder, for purposes which may include (but not be limited to):

- employee management, include the screening of curriculum vitae;
- individuals utilizing the Pple 's website; and
- business purposes, including communication by phone, fax, email, in person or other method of communication.

Pple may also, with consent from the data subject, collect personal information from third parties including:

- reference checks with referees; and
- through networking with peers.

3.4 The Purpose of Collection

Pple collects sensitive and personal information about stakeholders to carry out its business functions and fulfil its obligations. These may include (but are not limited to):

- the pursuit of legitimate business objectives;
- complying with government legislation (e.g.: Pple collects tax file numbers to comply with taxation requirements);
- meeting employment obligations to contractors and employees, which may include the processing of sensitive information (e.g.: sick leave).

In addition, Pple may occasionally be required by law to collect, use and disclose personal information, for example in order to comply with the requirements of government departments for business data, or in support of a criminal investigation.

3.5 Collection, Use and Disclosure of Sensitive/Personal Information

Pple may only collect, store, process or disclose personal data / information pertaining to an individual:

- if it is lawful to do so;
- by individuals authorised to do so in the course of their duties;
- with the knowledge of the data owner of the personal data / information, unless directed otherwise by legal authority; or
- either
    - with the express or implied consent of
        - the data owner;
        - guardian of the data owner of the personal data / information, or;

        - individual legally authorised to act on behalf of the data / information owner; or
    - in order to satisfy a legitimate commercial purpose; or
    - if required to do so meet a legislative or regulatory obligation.

Sensitive and Personal information may be disclosed to:

- staff of Pple responsible for administering the processes described above;
- health service providers in the event of the administering of emergency health services;
- related bodies and third parties for the administration and provision of selected benefits and services (e.g.: training or policy administration); and
- statutory authorities that may require sensitive data as per legislative requirements.

Pple may collect only the personal data / information that is required to effect the processing requirement.

3.6 Access, Correct or update Personal information

Pple must make reasonable attempts to ensure the accuracy of the personal data / information provided.

To the extent authorised by privacy legislation, Pple must provide data subject access to review and amend sensitive/personal information held by Pple. This may be for a reasonable administration fee, via existing communication channels.

3.7 Security of Sensitive and Personal information

Pple must take all reasonable steps to ensure that sensitive and personal information is held in a secure environment accessed only by authorised persons for approved business purposes.

However, no data processing can be guaranteed to be 100% secure. While Pple strives to protect all sensitive and personal information from misuse, loss and unauthorised access, Pple cannot guarantee the security of any information transmitted to and from a data source or recipient. Once a transmission is received, Pple will make the best effort to ensure its security in line with Pple data handling procedures.

3.8 Notifiable Data Breaches

Pple recognises the legislative requirements of the reporting of any breaches of personal or sensitive data / information.

As part of storing sensitive data / information, Pple accommodates data security within its ICT framework.

Pple will use its resources to the best of its capabilities to prevent any personal / sensitive information stored in its database being passed to unsolicited third parties. Unfortunately, Pple cannot provide a 100% guarantee that personal / sensitive information stored will not be obtained by unsolicited third parties.

In cases where Pple has evidence that personal / sensitive information has been obtained by unsolicited parties, Pple will:

- identify the cause of the breach;
- limit any further effects of any breach;
- remedy the breach;
- inform affected individuals;
- report any breaches to any relevant statutory authorities as required; and
- ensure Pple enacts any further processes depending on the nature of the breach.

3.9 Education and Awareness

Pple will incorporate the Privacy Policy into its induction pack, provide privacy training to staff dealing with personal data / information, and communicate privacy principles to all staff using awareness programs.

3.10 Privacy Enquiries

Data Subjects may contact the Data Privacy Office if they wish to:

- request access to, find out more about or seek amendment of personal data / information held by Pple;
- enquire generally about privacy rights and obligations;
- provide suggestions or feedback in respect of Pple's handling of personal information; or
- make a complaint in relation to Pple handling of personal information.

4 Responsibilities and Accountability

Below are high level functional Responsibilities of the Roles. Note that these can be, but do not have to be the same individual.

The Responsible Person for this Policy is the Information Officer. Pple reserves the right to monitor and audit networks and systems on a periodic basis, to ensure compliance with this policy.

4.1 The Board

- The Board is responsible for ensuring that Pple meets its legal, fiduciary, and business obligations to demonstrate compliance with global privacy related legislation (e.g. POPIA & GDPR), and other related privacy practices.
- The Board should provide the executive sponsorship of local and global privacy programs.

4.2 System Controller

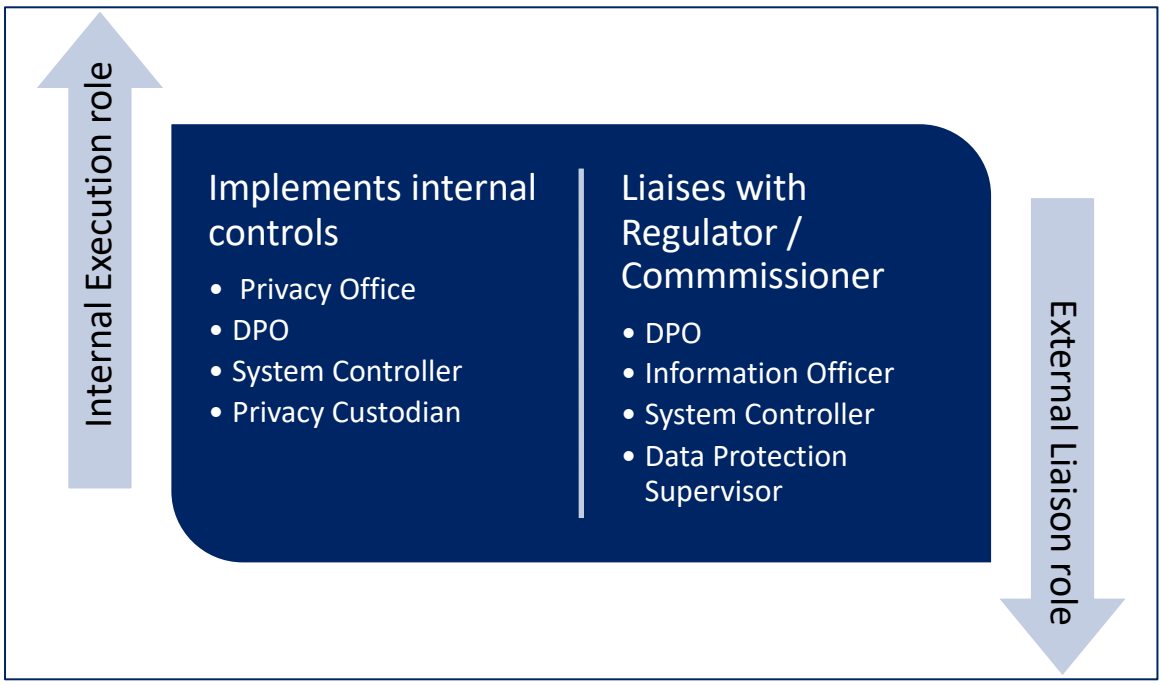
- Acts in accordance with the following Act pertaining to the Monitoring of indirect Communications: Regulation of Interception of Communications and Provision of Communication-Related Information Act, 70 of 2002 (RICA).
- Establishes internal processes for the requesting of monitoring of indirect communications, and ensures that key stakeholders utilise them.
- Validates the legitimacy of requests to perform monitoring in order to protect the right to privacy of the data subject, and to ensure Pple remains compliant with the law.
- Authorises or declines the monitoring request.
- Where the requests are authorized, set limitations on the extent and duration of the monitoring as appropriate.
- Perform assessments on occasion to ensure that monitoring limitations are adhered to.
- Keep records of all monitoring requests and their outcome.
- Liaise with Pple Legal as requested when evidence of monitoring approval is required for investigatory purposes.
- Liaise with authorities as required to provide evidence of the legality of monitoring operations.

4.3 Information Officer

- Establish the Privacy Office.
- Liaise with external legal advisor(s) as required.
- Define how to integrate "Privacy by Design" into system and product development.
- Maintain a data privacy incident/breach response plan.
- Maintain a breach notification protocol to affected data subjects.
- Maintain a breach reporting protocol to regulators, credit agencies, law enforcement.
- Identify ongoing privacy compliance requirements e.g., law, case law, codes, etc.
- Track and address global data protection issues identified through Privacy Impact Assessments (PIAs).

4.4 Implementation Staff

Pple has specific individuals tasked with ensuring compliance to Privacy Legislation. Note that there are two types of roles, which can be either fulfilled separately or by the same individuals.



4.4.1 Privacy Custodians

- Integrate Data Privacy into Business Risk Assessments.
- Maintain an inventory of personal data collected, retained and processed by Pple.
- Conduct due diligence around data privacy and security, including third party service providers and contractors, as well as potential vendors / processors / acquisitions.
- Training Pple employees on the relevant privacy/ compliance requirements.
- Promote awareness of this Policy.
- Identify and evaluate the company's data processing activities.
- To perform data protection impact assessments.
- Raise awareness and provide staff training for any employees involved with processing activities.
- Provide a repository of privacy information/monitoring requests.

4.4.2 Data Protection Officers/Supervisors

- Conducting regular assessments and audits to ensure compliance
- Responding to data subjects to inform them about how their personal data is being used and what measures Pple has put in place to protect their data
- Give advice and recommendations to Pple about the interpretation or application of the data protection rules.
- Provide advice regarding the data protection impact assessment and monitoring its performance.
- Handle complaints or requests by Pple, the data controller, data subjects, or introduce improvements on their own initiative.
- Ensuring that data subjects' requests to see copies of their personal data or to have their person data erased are fulfilled or responded to[2].
- Inform and advise Pple (data controller or data processor) and employees how to be Privacy compliant and how to comply with other data protection laws.
- To monitor Pple's compliance with Privacy legislation and any other applicable data protection provisions.

- To act as the focal point for the data protection supervisory authority on matters relating to the processing of personal data and other matters, where appropriate.
- Liaise with related stakeholders and teams as required
- Maintain policies, standards and guidelines for the collection and processing of personal information
- Maintain privacy notices on all relevant channels
- Facilitate privacy awareness
- Maintain documentation as evidence to demonstrate compliance and/or accountability

4.4.3 Security Representatives

Pple's Information Security Representatives will be responsible to ensure that the following requirements are met:

- Ensure that appropriate restrictions and controls are in place regarding authorised access (physical and logical).
- Committed to safeguard the Confidentiality, Integrity and Availability of all physical and electronic information assets in Pple to ensure regulatory, operational and contractual requirements are fulfilled.
- Ensure that the requirements in the Minimum Information Security Standard and related Policies are upheld at all times.

4.5 Employees

- Exercise good judgement regarding the appropriate use of Pple resources in accordance with Pple policies, procedures, standards and guidelines.
- Pple information assets and information must not be used for any unlawful or prohibited purposes.
- Any Pple data created by an Employee on an Pple system remains the property of Pple.
- Pple employees must take responsibility to familiarise themselves with, and adhere to the requirements of this Policy.
- Any Pple employee that processes Personal Information must always ensure and maintain the privacy of the Personal Information processed.
- Pple employees must notify the Information Officer in the event that a breach is identified.