ACCOUNTABILITY™

YOUR GATEWAY TO SAFER BUSINESS

ISP-024- Personal Information Protection Policy

June

2023

This document describes the Personal Information Protection Policy at Accountability[1] and is an integral part of the Quality Management and Information Security Management System and Manual.

Process/Policy Document

[1] "Accountability" hereby refers to Accountability Group (Pty) Ltd (registration number 2008/012163/07) and Accountability Solutions (Pty) Ltd (registration number 2017/365254/07), both companies incorporated in terms of the laws of South Africa, having its main place of business at 29 Bella Rosa Road, Rosenpark, Bellville, 7530 which it hereby elects as its domicilium citandi et executandi.

Table of Contents

Uncontrolled copy when printed

Document Control

Process / Policy Owner:	**Compliance Officer**
Process / Policy Number:	**ACC ISP-024 Personal Information Protection Policy**
Last Review Date:	**June 2023**
Next Review Date:	**June 2024**
Electronic Location:	**Apliso Plus System**

Quality Management System Requirements

All requirements to ensure that this procedure will ensure the security of confidential information have been defined and documented in this procedure and the documented Quality Management and Information Security Management System procedures:

- Risk Management Process
- ACCG-ADM-PRO003_Control_of_Documents_and_Records_Process
- ACCG-ADM-PRO004_Corrective_and_Preventative_Action_Process
- ACCG-ADM-PRO005_Control_of_Non-Conformance_of_Service_Process
- ACCG-ADM-PRO006_Internal_Audit_and_Management_Review_Process

1 Introduction

Given the nature of Accountability's business, which is providing services that contain Personal Information **(PI)** to clients via various platforms and, storing this sensitive member information on our internal systems, we must comply with international legislation such as the Protection of Personal Information Act **(POPIA)**, General Data Protection Regulation **(GDPR)** and Financial Regulatory requirements. This Policy, however, applies to any PI supplied to a third party for processing.

This legislation gives effect to the right to privacy and regulates the way PI may be processed by providing rights and remedies to protect PI. This applies not only to the processing of PI by a responsible person domiciled in the country, and where processing happens, but also to citizens of a different country/zone (for example EU citizens are protected by GDPR outside of the borders of the EU). Specific to POPI, the Act will override other legislation that contains inconsistent provisions relating to the processing of PI, and where other legislation provides for more extensive conditions for the processing of PI, the other legislation will prevail.

PI relates to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person, and includes, but is not limited to:

- Race, gender, pregnancy, marital status, national or ethnic origin, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language, and birth of a person.

Processing is any operation or activity, whether by automatic means, including:

- Collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation, or use.
- Dissemination by means of transmission, distribution or making available in any form.
- Merging, linking, as well as restriction, degradation, erasure, or destruction.

Key concepts include:

- "**Consent**" means any voluntary, specific, and informed expression agreeing to the processing of PI.
- "**Data Subject**" means the person to whom the PI relates.

2 Objectives and Scope

PI must be collected for a specific, explicitly defined, and lawful purpose related to the function or activity of the responsible party. The data subject must be made aware of the purpose of the collection.

Records must not be retained any longer than is necessary for achieving the purpose for which it was collected unless:

- Further retention is required by law;
- The responsible party reasonably requires to keep it;
- Retention is required by a contract between the parties;
- The data subject consents to further retention.

PI must be destroyed, deleted or de-identified as soon as is reasonably practical. Destruction or deletion must be done in a manner that prevents its reconstruction in any form.

- The Accountability employee shall ensure that the information collected will not be used for any other purpose before obtaining the individual's approval unless the new purpose is required by law.

- The Accountability employee shall ensure that a person collecting PI will be able to explain to the individual why this is being done.

- The Accountability employee shall ensure that limited collection, limited use, disclosure, and retention principles are respected in identifying why PI is to be collected.

3 Validity of this document

This document is valid from the last review date and authorised by the Management Representative and should be revised at least every twelve months or as required. This document replaces and supersedes all previously dated documents for this procedure, which are cancelled and destroyed.

4 Responsibilities for the process

The **Deputy Information Officers** are responsible to review a complaint submitted by a complainant who is dissatisfied with the conduct of his/her PI.

Information Officers' Accountability and Responsibility:

- Accountability's Directors will be appointed as Information Officers and the Compliance Officers will serve as the deputies.
- All persons who collect, process, or use PI shall be accountable to the Information Officers/Deputies for such information.
- Any person suspecting that the information is being used for purposes other than that explicitly approved and collected for may register a complaint with the Deputy Information Officer/s at disputes@accountability.co.za / ludwig@accountability.co.za
- The Deputy Information Officer/s shall investigate the above complaint and inform the complainant of his/her findings and corrective action taken, if any.
- If the complainant is dissatisfied with the findings of the Deputy Information Officer/s, an appeal may be submitted to Accountability's Information Officers. The determination made by Accountability's Information Officer/s will be final.
- The Deputy Information Officer/s shall be responsible to give training to all Accountability employees and other Partner(s) who might, collect, use, or retain PI.

5 Personal Information and consent process

- When collecting PI, the responsible party shall obtain consent from the Data Subject, to use, collect, retain, or disclose said PI.
- When collecting PI, the responsible party shall ensure that the Data Subject understand how the PI will be used.
- Express consent will be obtained from the Data Subject, unless it is in the Information Officer's opinion that implied consent will be acceptable. The consent must be clear and verifiable.
- The reasonable expectations of the Data Subjects will be respected.
- The Data Subject may, at any time, withdraw the consent given, subject to legal and contractual restrictions by giving reasonable notice.

6 Limiting collection and further processing process

The Responsible Party shall ensure that PI will not be collected indiscriminately, but by fair and lawful means, and be limited to what is necessary to fulfil the specific purpose for which the PI is being collected.

PI may only be processed if:

- The data subject consents to the processing;

- Processing is necessary for the conclusion or performance of a contract to which the data subject is a party;
  - There is a legal obligation to do the processing;
  - Processing protects the legitimate interests of the data subject;
  - Processing is necessary for the pursuit of the legitimate interests of the responsible party;

A data subject may object, at any time, on reasonable grounds, to the processing of their PI. The responsible party may then no longer process the PI.

PI must be collected directly from the data subject except if:

- The information is contained in a public record or has deliberately been made public by the data subject;
- The data subject has consented to the collection from another source;
- Collection from another source would not prejudice a legitimate interest of the data subject;
- Further processing must be compatible with the purpose for which it was collected unless the data subject gives consent to further processing.

7 Use of Personal Information for direct marketing

"**Direct marketing**" means unsolicited electronic communication.

The processing of PI for direct marketing by any form of electronic communication is prohibited unless the data subject:

- Has given consent; or
- Is a member of the responsible party and if:
  - The responsible party has obtained the contact details of the data subject in the context of the sale of a product or service;
  - It is for marketing the responsible parties' own similar products or services; and
  - If the data subject has been given a reasonable opportunity to object, free of charge, at the time the information was collected or on the occasion of each communication for the purpose of marketing.

A responsible party may only approach a data subject whose consent is required, and who has not previously withheld such consent, once, to gain consent and such consent must be in the prescribed manner and form.

8 Accuracy of Personal Information

A responsible party must take reasonably practical steps to ensure that PI is complete, accurate, not misleading and updated where necessary. The PI shall not be updated routinely unless it is required to fulfil the purpose for which the PI was collected.

9 Data and information safeguards

A responsible party must secure the integrity and confidentiality of the PI in its possession or under its control by taking appropriate, reasonable technical and organizational measures to prevent the loss, damage or unauthorized destruction, unlawful access to, or processing of the PI.

Anyone processing PI on behalf of a responsible party must:

- Treat the information as confidential and not disclose it unless required by law;

- Apply the same security measures as the responsible party;
- The processing must be governed by a written contract ensuring safeguards are in place; and
- If domiciled outside the Republic of South Africa, comply with local protection of personal information laws.

The Data Subject may request the responsible party to:

- Correct or delete PI that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully;
- Delete or destroy PI that the responsible party is no longer authorized to retain.
- The Deputy Information Officer shall ensure that all employees and consultants know the importance of keeping PI confidential. The Deputy Information Officer shall ensure that care is taken when PI is disposed of or destroyed to prevent unauthorized parties from gaining access to it.

10 Openness

The Deputy Information Officer must take reasonably practicable steps to ensure the Data Subject is aware of:

- The information being collected;
- The name and address of the Responsible Party;
- The purpose for which the information is being collected;
- Whether or not the supply of the information is voluntary or mandatory;
- The consequences of failure to provide the information;
- Any law authorizing the requiring of the collection;
- The right of access to, and the right to rectify the information collected;
- The fact that, where applicable, the responsible party intends to transfer the information to a third country/international organization and the level of protection afforded by that third country/organization; and
- The right to object to the processing of the information.

11 Individual's access to their Personal Information

The Deputy Information Officer/s shall, upon request, inform an individual whether Accountability holds PI about the requested party. If possible, the information's source shall also be given. Accountability shall allow the individual access to the information.

Accountability shall also account for the use that has been made or is being made of this information and give an account to the third parties to whom it has been disclosed. (Note, if the Deputy Information Officer/s believes for valid reasons that access to PI should be denied, the Deputy Information Officer/s shall consult legal counsel before making such a decision.)

A person requesting individual PI may be required by the Deputy Information Officer/s to give sufficient information to permit Accountability to provide an account of the existence, use, and disclosure of PI. Information shall be used only for the purpose for which it was obtained.

The Deputy Information Officer/s shall ensure that Accountability responds to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be made available in a generally understandable form. For example, Accountability shall explain abbreviations or codes it uses to record information.

The Deputy Information Officer/s shall ensure that when an individual successfully demonstrates the inaccuracy or incompleteness of PI, Accountability shall amend the information as required. Depending on the information challenged, amendment involves the correction, deletion, or addition of information in question.

The Deputy Information Officer/s shall ensure that when a challenge is not resolved to the individual's satisfaction, Accountability shall record the unresolved challenge's substance. When appropriate, the unresolved challenge's existence shall be transmitted to third parties having access to the information in question.

12 Risk Management

All risks identified and associated with this policy/procedure are recorded on the Risk Management Register *(Risk Management Register)* and managed according to the Risk Management Process *(ACCG-ADM-PRO002_Risk_Management_Process)*

13 Corrective Action

The company's ACCG-ADM-PRO004_Corrective_and_Preventative_Action_Process will be activated if this procedure fails to meet the desired objectives.

14 Updating and Distribution of this Document

The updating of this process can be initiated by the Process Owner following the procedure defined in the ACCG-ADM-PRO003_Control_of_Documents_and_Records_Process.

This policy can be updated at any time and when necessary, by the Information Officer.

This Policy should be reviewed on a continual improvement basis for suitability, adequacy, and effectiveness, or at least no less than every twelve months.

The distribution of this Policy is circulated to the following persons:

- Director(s)
- Information Officer(s)
- HR Manager
- Financial Manager
- Staff Members

15 Management Review

Management should review this document on a continual improvement basis for suitability, adequacy and effectiveness, and at least no less than every 12 months.

Reports required for the reviewing of input and output of this process are:

- Customer service delivery reports
- Customer Satisfaction Survey results
- Minutes of customer meetings
- Follow-up actions from previous management reviews
- Risk Management Register
- Information Security Incident Management Reports