PROTECTION OF PERSONAL INFORMATION POLICY (POPI)

FSP NAME	Groups Are Us (Pty) Ltd
FSP NUMBER	45735
FSP ENTITY	Credit Life And Funeral Cover Insurance
PHYSICAL ADDRESS	Groups Are Us Building 34 Newton Street Newton Park Gqeberha 6055
TELEPHONE NO	041 004 0114
POLICY DATE	March 2025
AUTHOR	Tinita Gerber

Contents

1. DEFINITIONS :

1.1 "**Consent**" means the permission required to collect and process personal information.

1.2 "**Data subject**" means – the person to whom the personal information relates.

1.3 "**Data breach**" means the personal information of a data subject has been lost, accessed or acquired by an unauthorised person which is likely to impact the data subjects rights to privacy and freedom.

1.4 "**Data Compromise**" refers to an incident where a data subject's personal information is lost, accessed, or obtained by an unauthorized party - however, such an incident is considered unlikely to pose a risk to the rights and freedoms of the data subject. This occurs due to a failure or compromise—whether caused by human actions, electronic interference, or inaction—that compromises the security of the information in our possession.

1.5 "**Personal Information**" means information relating to an identifiable living, natural person and where t is applicable, an identifiable, existing juristic person (including but not limited to the full list mentioned in clause 6). This is information relating to a person and includes all information about that person, including their characteristics and identifying information and correspondence that are implicitly or explicitly of a private or confidential nature.

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

1.6.1 The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

1.6.2 Dissemination by means of transmission, distribution or making available in any other form; or

1.6.3 Merging, linking as well as restriction, degradation, erasure or destruction of information

1.7 "**Record**" means any recorded information in whatever form in possession or under the control of the responsible party.

1.8 "**Responsible Party**" means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

1.9 "**Restriction**" means to withhold from circulation, use or publication of any personal information that forms part of a filing system, but not to delete or destroy such information.

1.10 **"Security Compromise"** refers to an incident where a data subject's personal information is lost, accessed, or obtained by an unauthorized party - however, such an incident is considered unlikely to pose a risk to the rights and freedoms of the data subject. This occurs due to a failure or compromise—whether caused by human actions, electronic interference, or inaction—that compromises the security of the information in our possession.

1.11 "**Special Personal Information**" means personal information as referred to in section 26 of this act

1.12 "**Unique Identifier**" means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

2. BACKGROUND

2.1 Groups Are Us (Pty) Ltd is a registered company and financial services provider rendering the following services to clients relating to personal / sensitive information:

2.1.1 Processing personal information of clients

2.1.2 Processing of personal information of beneficiaries

2.1.3 Processing personal information of employees and representatives (Natural and Juristic)
2.1.4 Processing of personal information of business partners (and their beneficial owners)
2.1.5 Remote business submission via or business and service providers
2.1.6 Client transactional record keeping

2.2 As Groups R Us makes use of and processes the above-mentioned personal information and therefore must comply with the Protection of Personal Information Act (POPI Act)
2.3 Services are provided in terms of contractual agreements and/or on request.
2.4 Groups R Us is based at 34 Newton Street, Newton Park, Port Elizabeth, 6045 and is solely owned and managed by shareholders represented by four directors.

3. PURPOSE

3.1 The purpose of this Policy is to ensure compliance with the Protection of Personal Information Act (POPI Act) as required by section 19(1) of that Act and aims to ensure that the security and confidentiality of personal data, processed by Groups R Us, is a matter of high priority and that all personal information under the control of Groups R Us will remain secure and protected.
3.2 This Policy therefore enforces legal obligations on responsible parties, such as Groups R Us' processing personal information on behalf of all data subjects.
3.3 The integrity and confidentiality of personal information processed on behalf of clients is a high priority for Groups R Us and will be secured and protected as documented in the paragraphs to follow.

4. SCOPE

4.1 This policy applies to all personal data processed and controlled by Groups R Us. The policy is available to all staff and clients.
4.2 This policy does not apply to the processing of personal information:
4.2.1 In the course of purely household or household activities
4.2.2 Solely for the purpose of journalistic, literacy or artistic expression, to the extent that such exclusions are necessary to reconcile, as a matter of public interest, the right to privacy with the right to freedom of expression.
4.2.3 By or on behalf of a public body
4.2.3.1 Which involves national security, including activities that are aimed at assisting in the identification of the financing of terrorists and related activities, defence or public safety; or
4.2.3.2 The purpose of which is the prevention, detection including assistance in the identification of the proceeds of unlawful activities and the combatting of money laundering activities, investigation or proof of offences, the prosecution of offenders or the execution of sentences or security measures. To the extent that adequate safeguards have been established in legislation for the protection of such personal information.
4.3 The regulator may grant further exemptions to comply with the conditions for lawful processing of personal information as stipulated in the POPI Act.
4.4 A copy of this policy will also be made available on the Groups R Us website.
4.5 Breaches of the POPI Act or regulation will be reported to the Information Regulator as required by Section 22 of this act.

5. POLICY

5.1 The POPI Act and regulations applies to both clients and processors.
5.1.1 The clients determine the purposes and means of processing personal data.

5.1.2 The data processor or responsible party is responsible for processing personal data on behalf of a client.

5.2 To comply with the POPI Act, Groups R Us must ensure that the data it collects
- 5.2.1 are processed fairly,
- 5.2.2 collected for legitimate reasons,
- 5.2.3 adequate for their purpose
- 5.2.4 accurate and up to date
- 5.2.5 deleted when no longer needed
- 5.2.6 processed and stored securely.

5.3 Groups R Us is committed to demonstrating how we take steps to comply with these principles.

6. WHAT IS PERSONAL INFORMATION?

6.1 The POPI Act defines personal data as any information that relates to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person who can be identified, directly or indirectly, from that information (the Data Subject).

6.2 The POPI Act defines personal information in Section 1. Personal data can include:
- 6.2.1.1 Names
- 6.2.1.2 Dates of birth
- 6.2.1.3 Location data
- 6.2.1.4 Email addresses/ telephone numbers
- 6.2.1.5 Addresses
- 6.2.1.6 Identification numbers
- 6.2.1.7 IP addresses
- 6.2.1.8 Pseudonymous data
- 6.2.1.9 Online identifiers

6.3 This includes genetic data, and biometric data where processed to uniquely identify an individual. Personal Information can include data about:
- 6.3.1.1 Health
- 6.3.1.2 Genetics (age/ race/ gender/ pregnancy/ national-ethnic or social origin/ physical or mental health / wellbeing / disability)
- 6.3.1.3 Biometrics
- 6.3.1.4 Sexual orientation or marital status
- 6.3.1.5 Trade union membership
- 6.3.1.6 Political opinions or beliefs
- 6.3.1.7 Culture and language
- 6.3.1.8 Religious or philosophical beliefs
- 6.3.1.9 Any identifying number, email, etc
- 6.3.1.10 Private correspondence and correspondence sent by the person that would reveal the contents of the original correspondence.
- 6.3.1.11 Education, financial, criminal or employment history
- 6.3.1.12 Personal opinion, views or preferences pf the data subject
- 6.3.1.13 The views or opinions of another individual about the data subject

7. ACCOUNTABILITY

7.1 As per section 8 of the ac, Groups R Us will at all times ensure that the conditions for lawful processing of personal information are complied with internally and through all external business partners due to the fact that Groups R Us will remain responsible for the processing of personal information regardless of it having passed the information on to a third party to process the personal information.

7.2 Groups R Us therefore expects all business partners to implement appropriate technical and organisational safeguards to meet the POPI Act requirements and protect the rights, freedoms and privacy of Data Subjects.

7.3 To ensure control over the processing of personal information, Groups R Us has identified all personal data collected and processed, both directly and indirectly. This information is documented in our POPI Information Processing Register, which is reviewed annually.

7.4 Groups R Us has appointed an Information Officer and two deputy Information Officers who are responsible for ensuring that all personal information being processed complies with the requirements of the POPI Act.

7.5 In summary, Sections 14 to 23 requires that Personal information should be:

7.5.1 accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

7.5.2 kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the POPI Act in order to safeguard the rights and freedoms of individuals; and

7.5.3 processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

7.5.4 Groups R Us intends to comply with the above requirements including all the other conditions 1 to 8 in Chapter 3 of the POPI Act.

8. LAWFULNESS OF PROCESSING

8.1 Groups R Us ensures that all personal information s processed in a lawful and reasonable manner that does not infringe the privacy of the data subject and therefore neither Groups R Us, nor our business partners or employees will act unlawfully in its collection or processing of personal information.

8.2 Groups R Us will at all times ensure that the processing of such personal information is done in a reasonable manner in line with the interests and expectations of the data subject.

8.3 Section 10 of the act requires that Groups R Us may only process the personal information of a data subject providing that the purpose for which it is processes is adequate, relevant and not excessive. Groups R Us may therefore only collect and process personal information if it is in line with the intended purpose communicated to the data subject at the time of data collection/ request.

9. LOCATION OF PROCESSING

20.2 All data processed by Groups R Us will be processed within the South African boundaries.

20.3 Groups R Us will not transfer personal data to territories outside South Africa without the explicit consent of the individual.

20.4 This also applies to publishing information on the internet, as data transfers include making information available on a website accessible from outside South Africa. Groups R Us will always obtain consent from clients or individuals before publishing any personal data (including photographs) on its website.

10. CONSENT

10.1 Where consent is relied upon as a legal basis for processing, Groups R Us will collect consent in a recorded and demonstrable manner.

10.2 Consent will be gathered in a way that is freely given, specific, informed and unambiguous. Groups R Us will make it explicitly clear to clients what they are giving consent for, and will process personal data on their behalf in a manner that is consistent with the consent the individual has given.
10.3 Consent does not have to be provided in writing, however taking it into consideration that Groups R Us bears the burden of proof that consent was given, we have made an internal requirement that all POPI consent should be obtained in writing.
10.4 The consent needs to be provided by the data subject directly and in the case of a child, a responsible competent person. The individual or client has to provide clear consent for you to process their personal data or data on their behalf for a specific purpose
10.5 The processing is necessary for a contract you have with the client, or because they have asked you to take specific steps before entering into a contract to which the data subject is a party.
10.6 The processing is necessary for you to comply with the law (not including contractual obligations).
10.7 The processing protects the legitimate interest of the data subject
10.8 The processing is necessary for the proper performance of a public law.
10.9 The processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
10.10 The processing is necessary for the legitimate interests of the data subject or the legitimate interests of a third party/ business unless there is a good reason to protect the individual's personal data which overrides those legitimate interest.
10.11 Where consent is relied on as a lawful basis for processing at Groups R Us, clients or individuals have a right to withdraw consent at any time.
10.12 Groups R Us will make it as easy for an individual to revoke consent as it was to grant consent and all marketing emails sent by Groups R Us will include an unsubscribe link.
10.13 The data subject may at any time object to the processing of his/her personal information on reasonable grounds relating to his/her particular situation, unless legislation provides for such processing or for purposes of direct marketing other than direct marketing by means of unsolicited electronic communication as referred to in section 69 of this act.
10.14 If the data subject has objected to the processing of personal information in terms of 9.13 above, Groups R Us, nor its business partners may further process such personal information.
10.15 As per section 12 of the Act, as far as possible Groups R Us will collect the personal information from the data subject directly except:
    10.15.1 Where the information is contained or derived from a public record or has deliberately been made public by the data subject.
    10.15.2 Where the data subject or a competent person where the data subject is a child has consented to the collection of information from another source
    10.15.3 Where the collection of information from another source would not prejudice the legitimate interest of the data subject.
    10.15.4 Where Collection of the information from another source is necessary-
        10.15.4.1 To avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offenses.
        10.15.4.2 To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue
        10.15.4.3 For the conduct proceedings n any court or tribunal that have commenced or are reasonably contemplated
        10.15.4.4 In the interest of National Security
        10.15.4.5 To maintain the legitimate interest of the business or third party to whom the information is supplied.

10.15.5 Where compliance would prejudice lawful purpose of collection
10.15.6 Where compliance is not reasonably practicable in the circumstances.

10.16 If the information is ever collected from a third party, the data subject should be made aware of the processing of the information and the purpose from which the information has been collected.

11. DATA RETENTION AND DELETION

11.1 Groups R Us will not retain or process Personal Data for longer than is necessary or for longer than any period agreed to by the client or Data Subject. Once the purpose for which the information is collected or processes has been achieved, Groups R Us will not retain that records any longer than necessary unless the retention of that personal information record id required or authorised by law.

11.2 As a general rule, data will be retained as long as a relationship exists between the client, and a maximum of 5 years; unless a contract between parties requires that the records be retained.

11.3 Section 18 of the FAIS Act requires that records like client transactions, complaints, cancellations and financial records be kept for five (5) years from the period of the last transaction.

11.4 Records of personal information may be retained for periods in excess of those specified above for historical, statistical or research purposes if the business has appropriate safeguards in place to prevent personal information from being used for other purposes.

11.5 Groups R Us agrees to destroy, delete or de-identify the clients the record of personal information as soon as possible after Groups R Us' is no longer authorised to retain the records.

11.6 The destruction, deletion or deidentifying of personal information record will be done in a manner that prevents its reconstruction in an intelligible form. Hard copies of personal information will be destroyed by means of a shredding machine and the shredded paper will be collected by Sappi on a monthly basis.

11.7 Following the deletion of Personal Data Groups R Us shall notify the client or Data Subject that the Personal Data in question have been deleted. Where applicable, Groups R Us shall also provide confirmation that the Personal Data have been destroyed in accordance with instructions issued by the client or Data Subject.

11.8 Groups R Us will restrict the processing of personal data/ information if :

11.8.1 The accuracy is contested by the data subject for a period enabling Groups R Us to verify the accuracy of the information.

11.8.2 Groups R Us no longer needs the personal information for achieving the purpose for which the information was collected or processed, but it has to be maintained for purposes of proof

11.8.3 The processing is unlawful, and the data subject apposes its destruction or deletion and requests the restriction of the use instead.

11.9 Where the processing of personal information is restricted, Groups R Us will inform the data subject before lifting the restriction on processing.

12. DATA PROCESSING

12.1.1 As a responsible party, Groups R Us will implement its own appropriate technical and organizational safeguards when data is collected, processed and stored on behalf of clients to ensure the rights, freedoms and privacy of data subjects.

12.1.2 As a responsible party, Groups R Us will only work with business partners who can provide sufficient guarantees to implement appropriate technical and organisational safeguards to meet the POPI Act requirements and protect the rights, freedoms and privacy of data subjects.

12.1.3 When processing sensitive personal data as per Sections 26 to 34 of the POPI Act, additional safeguards will be implemented.

12.1.4 Groups R Us will implement:

12.1.4.1 pseudonymisation and/or encryption of personal data where required;

12.1.4.2 measures to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data on behalf of clients;

12.1.4.3 measures to ensure the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident;

12.1.4.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;

12.1.4.5 appropriate policies and governance frameworks to ensure continued compliance.

12.1.5 All client-processor relationships will be documented and managed with contracts that mandate privacy obligations.

13. SECURITY SAFEGUARDS

13.1 Groups R Us will always ensure the integrity and confidentiality of all personal information that is in its possession or under its control to prevent-

13.1.1 The loss of, damage to or unauthorised destruction of personal information and;

13.1.2 The unlawful and unauthorised access to our processing of personal information.

13.2 Groups R Us will implement appropriate technical and organizational measures to protect personal data against accidental loss, alteration, disclosure or unauthorised access. These measures ensure a level of security appropriate to the risks presented by the processing and the nature of personal data being processed.

13.3 Groups R Us ensures that the processing of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law and does not violate the relevant provisions.

13.4 Groups R Us ensures that appropriate, reasonable technical and organisational measures are in place to-

13.4.1 Identify and document all reasonably foreseeable internal and external risks that may have an influence on the personal information in its possession or under its control;

13.4.2 Establish and maintain appropriate safeguards against the identified risks;

13.4.3 Regularly verify and obtain confirmation that the safeguards are effectively implemented;

13.4.4 Ensure that safeguards are regularly updated n accordance with newly identified risks or deficiencies that may influence the current safeguards.

13.5 Groups R Us has carefully considered and taken into account widely accepted information security practices and procedures relevant to the financial industry when determining appropriate safeguards to implement.

13.6 Groups R Us also conducts regular training sessions for our employees to ensure they understand the importance of POPI, the associated risks, and the security safeguards applicable to them.

14. PHYSICAL ACCESS CONTROL

14.1 As Groups R us allows external parties onto the premises, access is properly controlled. Groups R Us Ltd has implemented, but not limited to, the following measures to prevent the unauthorized access to data:

14.1.1 Only Groups R Us staff will have access to the premises via their assigned access tag or gate control button.

14.1.2 These access credentials will be deactivated immediately upon termination of employment.
14.1.3 A security alarm system is in place to restrict access to unauthorized individuals, ensuring that only Groups R Us employees can enter areas where personal information is processed within the office premises.
14.1.4 Access to areas where personal information is stored and processed is strictly limited to authorized personnel only, ensuring controlled entry to these secure spaces.
14.1.5 Employees will have biometric access only to the areas necessary for their roles. This measure ensures that employees cannot access information they are not authorized to view.
14.1.6 Slam locks have been installed as an extra security safeguard to prevent unauthorized individuals from gaining access to the premises.

15. ACCESS CONTROL (SYSTEMS AND ELECTRONC INFORMATION)

15.1 Groups R Us has implemented the following measures to prevent unauthorized access to data processing systems:
15.1.1 User rights are assigned based on role requirements to ensure access is granted only to authorized individuals.
15.1.2 User profiles are assigned in accordance with Groups R Us' Access Management Policy and Change Management Policy to maintain security and control over system modifications.
15.1.3 System access is secured through password protection, with password complexity requirements governed by the Access Management Policy. This includes mandatory quarterly password updates and the deactivation of inactive user accounts after 21 consecutive days of inactivity.
15.1.4 Hardware and software firewalls are utilized to protect systems against unauthorized access and cyber threats
15.1.5 Regular vulnerability assessments and penetration testing are conducted to identify and mitigate potential security risks.
15.1.6 Virus scanning tools are employed to detect and prevent malware threats.
15.1.7 Sensitive files transmitted internally or externally are encrypted and/or password-protected to ensure data security.
15.1.8 These measures are continuously reviewed and updated to align with industry best practices and regulatory requirements.

16. TRANSFER CONTROL

16.1 Groups R Us has implemented, but not limited to, the following measures, to ensure that personal data cannot be read, copied or modified during electronic transmission or during transportation or storage to disk. Additionally, to control and determine to which bodies the transfer of personal data provided by data communication equipment is allowed:
16.1.1 Documentation of recipients of data and the time periods for the provision of data including agreed deletion times
16.1.2 Disclosure of data in anonymous or pseudonymous form
16.1.3 Creation of an overview of regular request and delivery operations
16.1.4 During physical transport, careful selection of transport personnel and vehicles
16.1.5 Disk encryption
16.2 Groups R Us We implements standard written agreements with all business partners (including, but not limited to, agents, suppliers, service providers, microlending service partners, and funeral parlour business partners) before sharing any information with them. These agreements are established either through a Non-Disclosure Agreement (NDA) or as part of our standard contracts.

16.3 Within this written contract between Groups R Us and the relevant business partner the relevant processes for the processing and storage of personal information is clearly stipulated and agreed upon by both parties. All such business partners of Groups R Us is responsible for establishing and maintaining the required safety measures as such business partner may also be held accountable for any contravention of this Act.

16.4 Such business partner is to notify Groups R Us immediately where there are reasonable grounds to believe that the personal information of the data subject has been lost, accessed or acquired by any unauthorised person or an information breach has occurred.

16.5 As outlined in the PAIA manual, when client information is shared with non-business partners, such as other insurers—specifically when transferring client data from one insurer to another upon client request or consent for policy underwriting—Groups R Us will always take necessary measures to protect personal information. This includes encrypting the data to ensure that the receiving insurer can only view the purpose of the record (i.e., confirming that the client was contacted) while preventing them from using the identifiable information for their own purposes.

17. INPUT CONTROL

17.1 Groups R Us has implemented a comprehensive set of controls to ensure the accountability and security of personal data within its data processing systems. These measures allow for the tracking and verification of who has accessed, entered, modified, or removed personal data. The controls in place include, but are not limited to:

17.2 All input, modifications, and updates to personal data are automatically logged within our in-house policy administration system, Distro. This system maintains detailed audit trails to ensure transparency, enabling the company to review and verify all data changes at any given time.

17.3 Distro enforces strict data retention policies by preventing the permanent deletion of documents or personal information without senior staff authorization. This measure ensures that records are not inadvertently lost due to accidental deletions or unauthorized actions, thus maintaining data integrity and compliance with regulatory requirements.

17.4 Access to data input, modification, or deletion is strictly governed by a structured authorization framework. Permissions are assigned based on predefined roles and responsibilities, ensuring that only authorized personnel can make changes to specific datasets. This access control structure prevents unauthorized alterations and enhances data security.

17.5 Distro ensures complete traceability of all data interactions by logging actions under individual user accounts rather than general user groups. This granular level of tracking enhances security by providing clear accountability for any data input, modification, or deletion, allowing the company to identify the specific individual responsible for each action.

17.6 These measures collectively reinforce Groups R Us' commitment to data security, regulatory compliance, and the protection of personal information.

18. SAFEGUARDS FOR ACCIDENTAL DAMAGE

18.1 Groups R Us The company has implemented a range of protective measures to prevent the accidental destruction or loss of personal data. These measures include, but are not limited to, the following:

18.1.1 Advanced fire and smoke detection systems are installed throughout company premises to provide early warning in the event of a fire, reducing the risk of data loss due to fire-related incidents.

18.1.2 All critical electronic devices and data storage systems are connected to surge-protected power strips to safeguard against electrical surges that could cause data corruption or hardware damage.

18.1.3 Security alarm systems are in place to detect and alert personnel of any unauthorized access to restricted areas, ensuring that personal data remains protected from physical breaches.
18.1.4 Fire extinguishers are strategically placed in key locations to allow for prompt action in case of fire, minimizing potential damage to data storage and IT infrastructure.
18.1.5 Periodic testing of data recovery procedures is conducted to ensure that, in the event of data loss, recovery systems function effectively, minimizing downtime and data unavailability.
18.1.6 A comprehensive data backup and recovery strategy has been established, detailing procedures for creating, maintaining, and restoring data backups to ensure business continuity.
18.1.7 Critical data backups are stored securely off-site in a protected location to prevent loss in the event of on-site disasters, such as fire, theft, or system failures.
18.1.8 The company has developed an emergency response plan, which is integrated into the Occupational Health and Safety Policy, to provide structured guidance on responding to incidents that may compromise personal data security.

18.2 These measures are continuously reviewed and updated to align with best practices and emerging threats, ensuring the highest level of protection for personal data.

19. DATA SUBJECT RIGHTS

19.1 Data Subjects have certain rights in relation to their personal data processed by Groups R Us on behalf of clients. Those rights include;

19.1.1 The Right to Consent

19.1.1.1 All data subjects have a legal right to consent to whether or not their personal information is allowed to be collected, processed or stored by a company or another person, as stated in clause 10 above.

19.1.2 The Right of Access

19.1.2.1 Data Subjects have a legal right to access a copy of the personal information held about them. This must be supplied in a commonly used format (e.g. PDF, Excel or Word document).

19.1.2.2 Access to information requests may be made in accordance with Clause 20 below.

19.1.3 The right to rectification

19.1.3.1 Data Subjects have the right to have any inaccurate personal data rectified and, taking into account the purposes of the processing, to have any incomplete personal data completed.

19.1.3.2 Such a request will only be processed if it is submitted in writing and includes sufficient identification of the data subject.

19.1.3.3 Such request can be made where the personal information collected, processed, or held by Groups R Us is confirmed to be Inaccurate, irrelevant, excessive, out of data, incomplete, misleading or obtained unlawfully

19.1.3.4 Once the change has been affected Groups R us will provide the data subject with credible evidence in support of the information being corrected.

19.1.3.5 Groups R Us will ensure that we will communicate all such change of personal information to all responsible parties to whom the personal information has been disclosed, providing that the change in information has an impact n decisions that have been or will be taken in respect of the data subject.

19.1.3.6 The data subject will also subsequently be informed of such disclosure as necessary action taken as a result of the request.

19.1.4 The right to erasure

19.1.4.1 In some instances, Data Subjects have a right to request the erasure of their personal data without delay. These instances may include:

19.1.4.1.1 Where processing is no longer necessary;
19.1.4.1.2 Consent has been withdrawn where the legal basis for processing is consent;
19.1.4.1.3 the Data Subject objects to processing and there is a valid reason under Data Protection law;
19.1.4.1.4 processing is for direct marketing purposes, and the data have been unlawfully processed.
19.1.4.1.5 General exclusions from this clause may include where processing is necessary for a legal reason or for the exercise or defence of legal claims.
19.1.4.1.6 Such a request will only be processed if it is submitted in writing and includes sufficient identification of the data subject.

19.1.4.2 Once the change has been affected Groups R us will provide the data subject with credible evidence in support of the information being erased.

19.1.5 The right to restrict processing

19.1.5.1 In some instances data subjects have a right to restrict the processing of their personal data. These instances include: the data are inaccurate; processing is unlawful but the subject opposes erasure; the subject has objected to certain forms of processing but agrees to other forms, or the subject objects to processing but the organisation requires it for the exercise or defence of legal claims.

19.1.5.2 Such a request will only be processed if it is submitted in writing and includes sufficient identification of the data subject.

19.1.6 The right to data portability

19.1.6.1 The right to data portability gives individuals the right to receive personal data they have provided in a structured, commonly used and machine-readable format. It also gives them the right to request that their data are transferred to another service provider.

19.1.6.2 Such a request will only be processed if it is submitted in writing and includes sufficient identification of the data subject.

19.1.7 The right to object

19.1.7.1 Section 24 of the POPI Act gives individuals the right to object to the processing of their personal data. The right to object only applies in certain circumstances. Whether it applies depends on the purpose for processing and the lawful basis for processing. Individuals have an absolute right to object to data processing for direct marketing purposes.

19.1.7.2 Such a request will only be processed if it is submitted in writing and includes sufficient identification of the data subject.

19.1.8 Rights in relation to automated decision making and profiling

19.1.8.1 Individuals have the right not to be subject to the results of automated decision making, including profiling, which produces legal effects on them or otherwise significantly affects them. This is defined as a process where there is no human involvement in the decision-making process.

19.1.8.2 Such a request will only be processed if it is submitted in writing and includes sufficient identification of the data subject.

19.1.9 The Right of Notification of security Compromises

19.1.9.1 If Groups R Us believes or has determined that the personal information of a data subject has been lost, accessed or acquired by an unauthorised person or an information breach has occurred, Groups R us must notify both the regulator and the data subject, unless the identity of the data subject cannot be established.

19.1.9.2 Notification of Security Compromises will be done in accordance with Clause 21 below.

19.2 Groups R Us intends to comply with the above rights of individuals and will not take part in automated decision-making and profiling activities.

19.3 Groups R Us will make all reasonable efforts to ensure that individuals who are the focus of the personal data ,being the data subjects, are informed of the identity of the data controller, the purposes of the processing, any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.

19.4 Groups R Us will ensure that the reason for which it processed the data originally is the only reason for which it processes those data, unless the client or individual is informed of any additional processing before it takes place.

19.5 Groups R Us will not seek to process any personal data which are not strictly necessary for the purpose for which they were obtained. Forms for collecting data will always be drafted with this in mind. If any irrelevant data are given by individuals, they will be destroyed immediately.

19.6 Groups R Us will review and update all data on a regular basis. It is the responsibility of the clients or individuals giving their personal data to ensure that these are accurate, and each individual or client should notify Groups R Us if, for example, a change in circumstances means that the data need to be updated. It is the responsibility of Groups R Us to ensure that any notification regarding the change is noted and acted on.

19.7 Groups R Us undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements.

19.8 Groups R Us will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste). A log will be kept of the records destroyed.

19.9 Where consent is relied on as a lawful basis for processing at Groups R Us, clients or individuals have a right to withdraw consent at any time.

20. SUBJECT ACCESS REQUESTS (DATA SUBJECT ACCESS REQUESTS/DSARS)

20.1 If a data subject has reasonable grounds to believe that Groups R Us is processing their personal information or retains their personal data, they have the right to request Groups R Us to confirm, at no additional charge, whether or not Groups R Us holds personal information about him, her or it.

20.2 The data subject may request Groups R Us the record or description of the personal information about him, her or it held by Groups R Us, including information about the identity of all third parties, who have, or have had, access to such personal information-

20.2.1 Within a reasonable time

20.2.2 At a prescribed fee, as per 21.3 below.

20.2.3 In a reasonable manner and format; and

20.2.4 In a form that is generally understandable

20.3 Groups R Us reserves the right under Section 23 of the POPI Act to charge a reasonable fee to cover administration costs where Access Requests are manifestly unfounded or excessive. Such written estimate or fee will be communicated prior to the providing of the personal information.

20.4 In this event, Groups R Us will delay the release of data until the fee is paid in full. Groups R Us will comply with Access Requests within 30 days of receipt.

20.5 If Groups R Us provides the requested information, Groups R Us must advise the data subject simultaneously of his, her or its right in terms of Section 24 of the POPI Act, to request the correction of the personal information.

20.6 Access requests should be directed in writing to Groups R Us, 34 Newton Street, Newton Park, Port Elizabeth, 6045 and e-mail: compliance@groupsrus.co.za)

20.7 It is imperative that this section is read alongside the Groups R Us PAIA manual as Groups R Us has the responsibility to, at all times, comply with the provisions of Par 2 and Part 3 of Chapter 4 of the Promotion of Access to Information Act (PAIA), prior to disclosing information to the data subjects to consult with the compliance department to establish whether the personal information being required data subject, does not have a restriction or partial restriction prior to it being disclosed.

20.8 Such a request will only be processed if it is submitted in writing and includes sufficient identification of the data subject.

21. BREACH & NOTIFICATION

21.1 In the event of a data breach involving personal data, Groups R Us will notify the Information Regulator promptly and without undue delay.

21.2 Notice is not required if the breach is unlikely to result in a risk to the rights and freedoms of individuals or clients.

21.3 Where feasible, the Information Regulator will be notified no later than 72 hours after Groups R Us becomes aware of the breach.

21.4 Where this timeframe cannot be met, Groups R Us will provide a reasoned justification for the delay.

21.5 Groups R Us will only delay notification to the data subject if a public body responsible for that prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.

21.6 Groups R us will take into account the legitimate needs of law enforcement or any measure reasonably necessary to determine the scope of the compromise and to restore the integrity of the business' information system.

21.7 Groups R Us will notify the data subject in writing and ensure that this communication reaches the data subject in at least one of the following ways:

- 21.7.1 Mailed to the data subjects' last known physical or postal address
- 21.7.2 Sent by e-email to the data subjects' last known email address
- 21.7.3 Placed in a prominent position on the website of the business
- 21.7.4 Published in the news media ; or
- 21.7.5 As may be directed by the Regulator

21.8 Groups R Us will ensure that the written notification provides sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise including-

- 21.8.1 A description of the possible consequences of the data breach
- 21.8.2 A description of the measures Groups R Us intends to take or has taken to address the data breach
- 21.8.3 A recommendation with regards to the measures to be taken by the data subject to mitigate the possible adverse effects of the data breach
- 21.8.4 If known to Groups R Us, the identity of the unauthorised person who my have accessed or acquired the personal information.

21.9 If an individual or client believes that Groups R Us' processing activities violate data protection laws, they have the legal right to file a complaint directly with Groups R Us. If the issue remains unresolved to their satisfaction, they may escalate the complaint to the appropriate supervisory authority. In South Africa, the governing body responsible is the Information Regulator.

22. DUTIES AND RESPONSIBILITIES OF THE INFORMATION OFFICER

22.1 As per Section 55 and 56 of the Act, Groups R Us has appointed and registered our Information officer and two deputy information officers whose responsibilities include-

22.1.1 The encouragement of compliance by the business, with the conditions for the lawful processing of personal information;
22.1.2 Dealing with requests made to the business pursuant to this Act;
22.1.3 Working with the regulator in relation to investigations conducted pursuant to chapter 6 of this Act on relation to the business of Groups R Us;
22.1.4 Ensuring compliance by the business with provisions of this Act.

22.2 Groups R Us will take into account Section 17 of the PAIA for the-
22.2.1 Appointment of such number of persons, if any, as Deputy information officers as necessary to perform the duties and responsibilities of the information officer and ;
22.2.2 Any power or duty conferred or imposed on the information officer by this Act, will be bestowed on such Deputy Information Officer(s) of Groups R Us.

22.3 The Information Officer of Groups R Us is the COO, duly authorised by the business and can be contacted on the following email address – andre@groupsrus.co.za .

22.4 The Deputy Information Officers are the Internal Compliance Officers of Groups R Us – and can be contacted on the following email address - compliance@groupsrus.co.za .

22.5 Groups R Us maintains this POPI Policy indicating all information processing operations within Groups R Us which is done in accordance to Section 14 and 51 of the PAIA Act.

22.6 Groups R Us may be charged with an administrative fine or the appropriate Information Officer and Deputy information officers may be criminally charged in the event that a section or sections of this act is contravened.

23. ENFORCEMENT AND PENALTIES

23.1 Any contravention and/or dispute in terms of this Act may be logged by the Information regulator, which possesses the authority to lodge an investigation and subsequently issue information-, enforcement – and infringement notices.

23.2 IF Groups R Us receives an information or enforcement notice, Groups R us reserves the right to lodge an appeal to the High Court having jurisdiction for the setting aside or variation of the notice, within 30 days after receiving the notice.

23.3 A data subject is not limited to lodge a complaint only to the Information Regulator, but may decide to institute civil action for damages in a court having jurisdiction against a responsible party for breach of provisions of this act, whether or not there is intent or negligence on the part of Groups R Us.

23.4 A court order issuing any order for damages must order it to be published in the Gazette and by such other appropriate public media announcement as the court considers appropriate.

23.5 Should Groups R Us, or any of its responsible parties (i.e business partners) be convicted pf an offense in terms of this Act, Groups R Us and the responsible party will be held liable to-
23.5.1 A fine or to imprisonment for a period not exceeding 10 years, or to both a fine and such imprisonment in the following circumstances:
23.5.1.1 Obstruction of Regulator [as per S100]
23.5.1.2 Failure to comply with enforcement notice [as per S103(1)]
23.5.1.3 False Evidence given by witnesses under oath [as per S104(2)]
23.5.1.4 Unlawful acts by the business in connection with account numbers [as per S105(1)]
23.5.1.5 Unlawful Acts by third parties in connection with account numbers [as per S106]

23.5.2 To a fine or imprisonment for a period not exceeding 12 months, or to both a fine and such imprisonment in the following circumstances:

23.5.2.1 Failure to notify processing subject to prior authorisation [as per S59]

23.5.2.2 Breach of Confidentiality [as per S101]

23.5.2.3 Obstruction of Execution of warrant [as per S102]

23.5.2.4 Failure to comply with information notice [as per S103(2)]

23.5.2.5 Witness failing to comply with the terms and conditions of the summons.

23.6 The amount of an administrative fine that may be imposed on Groups R Us by the Information Regulator may not exceed R10 million.

24. DOCUMENT REVIEW

This policy will be reviewed at least annually.