POPIA Policy

Contents

VERSION CONTROL

Document Information

Document Type: Policy
Applies To: THE REAL GROUP OF COMPANIES
"REAL GROUP"
Policy Owner: Compliance Officer
Effective Date: 01 Nov 2021
Current Version: 2021 V1.1
Review Frequency: Every 12 months

Version History and Approval

Version	Date Published	Prepared By	Reviewed By	Approved By	Last Review Date	Next Review Date
1.0	01 Nov 2021	Compliance Officer	Compliance Officer	Compliance Officer	01 Nov 2021	01 Nov 2022
1.1	01 Nov 2021	Senior Manager	Senior Manager	Senior Manager	01 Nov 2021	01 Nov 2022

Approval Status

This policy has been prepared, reviewed, and approved in accordance with the organisation's governance framework.

Details of preparation, review, and approval are recorded in the Version History and Approval table above.

Governance Note

Where segregation of duties is not reasonably practicable due to the size of the organisation, the same role may prepare, review, and approve a policy. This will be reassessed as the organisation grows.

Document Control Notice

This is a controlled document. Unauthorised copies are not valid.

The latest approved version of this policy is maintained in the official document management system.

Confidentiality Classification

Classification: Public Policy

Contact Information

For questions relating to this policy, please contact:

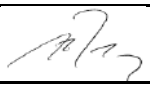
Compliance Officer
info@realhomefinance.co.za

POLICY STATEMENT

The organisation's Governing Body, its employees, volunteers, contractors, suppliers and any other persons acting on behalf of the organisation are required to familiarise themselves with the policy's requirements and undertake to comply with the stated processes and procedures.

POLICY ADOPTION

By signing this document, I authorise the organisation's approval and adoption of the processes and procedures outlined herein.

Name & Surname	Francois Rosslee
Capacity	Managing Director
Signature	
Date	1/11/2021

1. INTRODUCTION

The REAL Group provides and/or plan to provide financial services, including

- Housing finance, comprising mortgage loans and pension-backed loans;
- Advice on insurance, both long-term and short-term;

and hence continually has access to and needs to process personal data and information relating to individuals. This policy sets out how such personal data shall be processed, handled and stored to meet the data protection standards of the REAL Group and to comply with the Protection of Personal Information Act ("POPIA").

This POPIA Policy seeks to ensure that REAL Group:

- Complies with international legal standards and best practice for the receipt, importing, processing, handling and storing of personal data of individuals, both as received from its clients and customers, and as held in respect of its own employees;
- Protects the rights of its own employees, as well as that of its clients, customers and third parties in respect of individuals' data;
- Transparently renders how it processes, handles and stores individuals' data;
- Protects itself from the risks of a data breach.

2. APPLICATION

This policy applies to all employees of REAL Group in respect of all personal data accessed in the provision of services by REAL Group to its clients and customers, as well as the management of its employment relationships with its own employees.

It further applies to all data that it holds relating to identifiable individuals, including, but not limited to the following:

- names of individuals;
- physical addresses;
- postal addresses;
- email details;
- all telephone and mobile phone numbers;
- salary and other income; pension benefits; property value; credit rating; and all other data and information relating to an individual received in the course of providing services to such customer.

3. PROTECTION

This policy seeks to protect REAL Group from various very real data security risks including breaches of confidentiality through data breaches, hacking risks, and the risks of liability in relation to its clients, customers, third parties' data acquired from such clients and all its own employees.

The rules and standards set out in this policy applies regardless of:

- whether personal data relates to a client, customer or an employee of REAL Group, and/or
- is stored electronically, digitally, on paper, or on other materials, or through other methods.

4. GENERAL RULES RELATING TO PERSONAL DATA

Personal data shall at all times be:

- processed fairly and lawfully, in accordance with legal standards applicable to such data or data categories;
- obtained only for specific lawful purposes;
- adequate, relevant and not excessive;
- accurate, and kept up to date;
- held for no longer than necessary for the purpose it was obtained for;
- processed in accordance with the rights individuals;
- be protected in appropriate ways, methodologies and procedures and according to suitable methods, both organisationally and technologically;
- not be disclosed or transferred or exported illegally, or in breach of any agreement with a client or customer.

5. RESPONSIBLE PARTIES

All employees shall continually be responsible for ensuring the safeguarding, protection and avoidance of any unauthorised disclosure or breach of personal data in the execution of employment duties and services to REAL Group, or otherwise in the course of rendering services or being associated with the REAL Group.

6. THE INFORMATION OFFICER

The Managing Director acts as Information Officer and ensures compliance with the POPIA. In particular, the Information Officer shall:

- be registered with the Information Regulator;
- ensure that all operational and technological data protection standards are complied with;
- arrange data protection training and provide advice and guidance to all employees;
- be entitled and have authorisation to initiate disciplinary proceedings against any employee who at any time breaches any technological and/or organisational and/or operational data protection standard, rule, custom, instruction, policy, practice and/or protocol (verbal, in writing or otherwise) (“rule”) applicable in any department or area of the operations of the company;
- review and approve any contracts or agreements with third parties to the extent that they may handle or process data subject information;
- evaluate and approve requests from individuals to access data REAL Group holds about them “data subject requests”).

7. IT SERVICE PROVIDER

The IT Service Provider shall:

- ensure that all system services and equipment used for processing and/or storing data adhere to internationally acceptable standards of security and data safeguarding, and is regularly updated to continue to comply with such standards;
- issue appropriate, clear, regular rules and directives, including password protocols, data access protocols, levels of persons who enjoy access to certain data sign-on procedures, password safeguarding protocols, sing-on and sign-off procedures, log-on and log-off procedures; the

description of accessories, applications and equipment that will or may be used, and/or that may not be used under any circumstances, and the like.
- evaluate any third-party services the company is considering or may acquire to process or store data, e.g. cloud computing services.

8. GENERAL DATA PROTECTION RULES

All personal data shall be deemed confidential information, and be handled as such.

The only person/s entitled to access data covered by this policy, will be those who need to access it for the execution of their direct work services or required outputs.

Under no circumstances will data or personal information be shared outside the scope of required work. In the event of any doubt, an employee shall be entitled to access confidential information only after obtaining authorisation from their line manager or a senior manager, where any work output requiring access is unusual or out of the ordinary. Employees will receive induction and on-the-job training in relation to all security standards applicable to such employee's service delivery and work outputs involving personal information of individuals.

Employees shall keep all data secure by taking sensible practical precautions and complying with all rules, practices and protocols:

- In particular, strong passwords shall be used at all times;
- Passwords shall not be shared under any circumstances.

9. DATA STORAGE: PAPER

Where data is stored on paper, it will always be kept in a secure place where an unauthorised person cannot access or see it. This also applies to data stored electronically which has been printed out for some reason.

When not being processed, such papers should be kept in a locked drawer, safe or cabinet. Employees should ensure that paper and print outs are not left in places where unauthorised persons can see them, e.g. on a printer, and all unwanted paper must be shredded.

10. DATA STORAGE: ELECTRONIC DATA

Where data is stored electronically, it must be protected from unauthorised access, accidental deletion or any risk of exposure to malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly.
- All data will only be stored on designated drives and servers and shall only be uploaded to approved cloud computing services;
- All servers containing personal data will be located in secure protected locations away from general office space;
- Data will be backed up frequently in accordance with backup protocols. Such backups will be tested regularly in line with the company's standard backup procedures and protocols under the direction of the IT Manager. The Information Officer is responsible to schedule a minimum of two random tests each year;
- Data will never be saved directly to laptops or other mobile or removable devices such as tablets or smart phones or sticks or data sticks;

- All servers and computers containing data will be protected by approved security software, and one or more firewalls under the direction of the IT Manager.

11. DATA USE

It is acknowledged that personal data is at the greatest risk of loss, breach of confidentiality, corruption, hacking or theft when it is accessed or used. Therefore, when working with personal data, employees should ensure that screens of their computers are always locked when left unattended.

Personal data will not be shared informally, and in particular it will never be sent by email or without protection with appropriate passwords, where required to be sent by email.

Data shall be encrypted before being transferred electronically. The IT manager together with the Information Officer will develop and maintain protocols for data transfer to ensure it is sent in protected form to authorised external contacts only, and to avoid it being sent to any unauthorised external or internal parties.

Personal data shall never be transferred or sent to any entity not authorised directly to receive it.

Employees are prohibited from saving copies of personal data to their own computers.

Employees will at all times access and update only the central, official copy of any data or work output document, such as payroll.

Personal data is not of value to REAL Group, unless the business makes use of it in the course of providing services to its clients or customers, or administering its own employment relationships with employees.

12. DATA ACCURACY

Employees shall take reasonable steps to comply with company rules and work practices to ensure data is kept accurate and up-to-date.

The more important the accuracy of any component of personal data is, the greater the effort and measures will be to ensure its accuracy.

Data will always be held in as few places as necessary to ensure efficient service delivery and risk avoidance. Employees are not permitted to create any unnecessary additional data sets.

Employees will make use of every opportunity to ensure that a data component is accurate and up-to-date, e.g. by confirming details when handling a client call.

Employees shall at all times remain knowledgeable and informed about all data updating practices and work protocols used by REAL Group, such as updating via official, acknowledged websites and platforms used by clients.

13. INFORMATION ACCESS REQUESTS

Employees and individuals who are the subject of personal data held by REAL Group are entitled to:

- enquire what information is held about them and the purpose for holding it;
- enquire how to gain access to their own personal data;
- be informed of any special measures the company uses to keep such data up to date.

Information Access Requests shall be made by e-mail and addressed to the Information Officer, who shall address it in consultation with management.

The identity of a person making a data subject request will always be verified before handing over any information requested.

14. PROVIDING INFORMATION

In certain circumstances, South African legislation will allow that personal data be disclosed to law enforcement or other agencies without the consent of the individual. In such circumstance, REAL Group may be obliged to disclose the requested data, but will first ensure that the request is legitimate and will seek assistance beforehand from its legal advisers or other experts. Only the Information Officer will be authorised to furnish the requested data to the enquiring party.

15. DISCIPLINARY CODE AND INCORPORATION OF THIS POLICY INTO THE EMPLOYEE'S EMPLOYMENT CONTRACT

This data protection policy governs every employee of REAL Group, both during the course of his/her services to it, and to the extent applicable, after termination of services.

To the extent that this policy sets out workplace rules (as defined) governing the employee in the course of his/her work and services to the company, it shall form part of the company's Disciplinary Code and Procedure and is hereby also incorporated into it.

A breach of any rule in relation to the protection of personal data set out in this policy shall, in the event of breach thereof, form the basis of disciplinary action. In appropriate circumstances a breach hereof proven in a disciplinary enquiry may lead to dismissal.

The imposition of any disciplinary sanction or dismissal shall not preclude the company from instituting civil proceedings against an employee who acted in breach of this policy where such breach has resulted in liability, loss, reputational damage and/or other damages to the company in the course of pursuing its commercial operations.

It is incumbent upon every employee to familiarise him/herself with the content of this policy, and to remain up to date as to any changes to it issued in written form as part hereof by the company.

16. CHANGE LOG

Version	Section	Description of Changes	Reason
1.1	Entire document	Policy transferred to new company letterhead with no changes to policy content or intent	Corporate rebranding