PROTECTION OF PERSONAL INFORMATION POLICY

Version	Date of approval	Forum of Approval	Review period	Author
2.1	8 November 2023	ECL Board	Annual	Fanie van Biljon
2.2	12 November 2024	ECL Board	Annual	Fanie van Biljon
2.3	04 November 2025	ECL Board	Annual	Thuso Ndaba
2.4	01 June 2026	ECL Board	Annual	Thuso Ndaba

POLICY CHECKLIST

_____

Policy Owner:

Date:

POLICY CONTENT/SUBSTANCE CHECKLIST				
Have the following factors been considered:		**Yes**	**No**	**Comments**
1	Is the policy still relevant to our goals and mission?	X		
2	Do the objectives need to be updated and redefined?		X	
3	Does the policy comply with all relevant laws, regulations, and industry standards?	X		
4	Has input from affected or interested parties been obtained?	X		
5	Has the Policy been effective in achieving its intended outcomes?	X		
6	Are there any performance metrics or key performance indicators that can help assess the effectiveness of the policy?	X		
7	Is the policy still relevant to the current business environment?	X		
8	Are there any emerging risks that the policy should address?		X	
9	Does the policy adequately mitigate existing risks?	X		
10	Does the policy align with our values and culture?	X		
11	Does the policy conflict with any other policies and procedures within the group?		X	
12	Is the policy written in such a way that is easily understood by those who need to follow it?	X		
13	Are there any challenges or issues implementing and enforcing the policy?		X	
14	Are resources allocated appropriately?	X		
15	Have employees and relevant stakeholders been adequately trained and informed about the policy?	X		
16.	Does the policy have policies for feedback and reporting related to the policy?			N/A
17.	If you answered yes to question 16 above, have those mechanisms been reviewed?			N/A
18	If you answered no to question 16 above, are there mechanisms that can be implemented?			N/A
19	Is the policy cost effective, or are there ways to achieve the same objectives more efficiently?	X		
20	Is the review interval of the policy sufficient?	X		

21	Has the process been defined to implement policy changes?			N/A
22	Has the policy been reviewed and approved by the relevant committees?	X		
23	Have you considered what actions should be taken in the event of unforeseen circumstances or emergencies that may impact the policy?	X		
24	Is the policy intended to apply at Group level or to a specific entity?			Group Policy
25	Is there record on BaseCamp showing evidence of where the policy review has been discussed in detail, feedback gathered, and where the effectiveness of the policy changes after implementation can be monitored? If “No”, please create it. If “Yes”, please provide the BC link in the comments section.	X		https://3.basecamp.com/5304314/buckets/28714923/messages/9165214594

_____

Policy Owner:

Date:

1. Introduction

1.1 The right to privacy is an integral human right recognised and protected in the South African Constitution and the Protection of Personal Information Act 4 of 2013 ("POPIA" or "the Act').

1.2 Through its business activities, the Group is necessarily involved in the collection, use and disclosure of certain aspects of the personal information of clients, customers, employees and other stakeholders.

1.3 A person's right to privacy entails having control over his or her personal information and being able to conduct his or her affairs relatively free from unwanted intrusions.

1.4 Given the importance of privacy, we are committed to effectively managing personal information per the provisions of POPIA, other data privacy legislation and international best practice standards.

1.5 We will conduct periodic assessments in respect of personal information to ensure that we adhere to our obligations.

2. Definitions

2.1 In this policy, the terms below shall have the meanings as defined in the Act and cognate expressions shall have corresponding meanings;

2.2 "**client**" means any person or entity to which the Group provides a product or service including, but not limited to, debtors', policyholders and third-party credit providers. For purposes of this Policy, clients include potential and existing clients.

2.3 **"operator"** means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party;

2.4 "personal information"

means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—

(*a*)information relating to the 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, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

(*d*)the biometric information of the person;

(*e*)the personal opinions, views or preferences of the person;

(*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; and

(*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;

2.5 **''processing''** means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including—
(a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
(b) dissemination by means of transmission, distribution or making available in any other form; or
(c) merging, linking, as well as restriction, degradation, erasure or destruction of information;

2.6 "**the Group, "We**", "**Us**" means Evolution Credit Limited, its subsidiaries, affiliate and associate companies.

3. Scope

3.1 The policy applies to:

3.1.1 All personal information used, transformed or produced by the Group.

3.1.2 Any person in the employ of the Group or otherwise tasked by the Group and involved in the processing of personal information.

3.1.3 All departments, employees, service providers, contractors and other third parties who have access to personal information. In so far as any 3rd party processes personal information for, or on behalf of Us an "Operator Agreement" must be entered into with such 3rd party as POPIA requires this.`

3.2 Where required business and service channels must, subject to this policy, develop standard operating procedures to ensure the implementation of and compliance with the principles as set out in this policy. A register of all standard operating procedures will be kept, and all standard operating procedures are subject to approval by the relevant governance forum.

3.3 This policy does not apply where we act as operator and are required to adhere to such policies as may be prescribed by the third party unless such requirements conflict with this policy in which case this policy must be complied with.

3.4 This policy must be read in conjunction with the following Group policies (in the event of a conflict, this policy must be complied with);

3.4.1 Data Classification Policy

3.4.2 Back-up and Retention Policy.

3.4.3 Disaster Recovery and Business Continuity Policy

3.4.4 IT Security Policy

3.4.5 Promotion of Access to Information Manual

4. Personal Information Collected

4.1 The Act states that "Personal Information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive."

4.2 We collect and processes personal information about clients' financial position and/or needs. The type of information will depend on the type of client, e.g. credit and/or insurance, the need for which it is collected and will be processed for that, or a related purpose only, unless the client consents otherwise.

4.3 We will compile and update an inventory of information collected and processed by the Group.

4.4 Where we collect special personal information, we will, where required, obtain consent from the data subject.

4.5 As far as reasonably practicable we will collect information directly from data subjects. Where this is not possible, information may be collected from other sources as provided for in this policy. We will, as far as reasonably possible, keep record of the source of any personal information we collect.

4.6 Examples of personal information we collect, and process include, but is not limited to:

4.6.1 The Client's Identity number, name, surname, address, postal code, marital status, and number of dependants;

4.6.2 Description of the client's residence, business, employment, assets; financial information, banking details, etc;

4.6.3 Any other information required by the Group, suppliers and Insurers to provide clients with the goods and services which forms part of the Group's business being financial services related to long term insurance, the provision of credit and debt collection.

4.6.4 We are further obliged to process certain information as required in terms of Financial Sector laws, including, but not limited to, The Financial Intelligence Centre Act, The National Credit Act, The Financial Advisory and Intermediary Services Act.

4.7 We also collect and processes personal information for marketing purposes to ensure that our products and services remain relevant to our clients and potential clients.

4.8 The Group will have agreements in place with all product suppliers, insurers and third-party service providers to ensure a mutual understanding concerning the protection of personal information. Suppliers will be subject to the same regulations as applicable to the Group.

4.9 We may also supplement the information provided with information we receive from other providers to offer a more consistent and personalised experience in the data subjects' interaction with the Group and to ensure that personal information is kept accurate and up to date.

4.10 We will notify clients, where reasonably practicable, in relation to the information which we collect and how we will process and safeguard the information.

4.11 Where the Group collects information related to children, the competent person will be required to confirm that he/she is authorised to provide the information to us, unless the processing is justified as provided for in terms of the Act.

5. The Use of Personal Information

5.1 The Client's Personal Information will be used for the purpose for which it was collected or obtained.

5.2 In certain instances will attempt to obtain consent to process information, where this is not possible, we will process information only for the purpose it was obtained and will cease processing if compelled to do so as per the provisions of the Act.

5.3 The purpose for which we use personal information may include the following;

5.3.1 Providing products or services to clients and conclude transactions as requested;

5.3.2 Assessing and processing claims and or queries;

5.3.3 Conducting credit reference and affordability assessments;

5.3.4 Confirming, verifying and updating client details;

5.3.5 Enforcing our legal rights;

5.3.6 Debt collection and credit management;

5.3.7 For the detection and prevention of fraud, crime, money laundering or other malpractices;

5.3.8 Conducting market or customer satisfaction research;

5.3.9 Providing clients with updates in respect of our product offering/s.

5.3.10 For audit and record-keeping purposes;

5.3.11 In connection with legal proceedings;

5.3.12 Providing services to clients, to render the services requested and to maintain and constantly improve the relationship;

5.3.13 Providing communication in respect of the Group and regulatory matters that may affect data subjects; and

5.3.14 In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law

5.4 We will only process personal information if one or more of the following conditions are met;

5.4.1 with consent;

5.4.2 where the processing is necessary to enable us to perform our duties or enforce our legal rights;

5.4.3 processing complies with an obligation imposed by law;

5.4.4 processing protects a legitimate interest of the client, it is in the client's best interest to

5.4.4.1 have a full and proper assessment performed to provide them with an applicable, beneficial and affordable product or service; or

5.4.4.2 assist clients with debt to meet their financial obligations, and support our clients on their journey to become financially independent; or

5.4.4.3 assist clients in obtaining appropriate life insurance products and cover.

5.4.5 Processing is necessary for pursuing our legitimate interests or those of a third party to whom information is supplied — in order to provide data subjects with products and or services both we and any of our product suppliers require certain personal information from the customers to make an expert decision on the unique and specific product and or service required.

6. Disclosure of Personal Information

6.1 We may disclose personal information to any of our group companies or subsidiaries, joint venture companies and or approved product- or third-party service providers whose services or products data subjects elect to use, subject to agreements being in place to ensure that compliance with confidentiality and privacy conditions.

6.2 We may also share personal information with and obtain information about data subjects from third parties for the purposes listed above.

6.3 We may also disclose information where we have a duty or a right to disclose in terms of applicable legislation, the law, or where it may be deemed necessary in order to protect our rights.

6.4 We may disclose personal information we collected to our shareholders, funders or third-party service providers, with whom we engage in business or whose services or products we elect to use.

As far as reasonably possible we will enter into written agreements to ensure that other parties comply with our confidentiality and privacy requirements.

7. Third-Party Risk Management (Service Provider/Suppliers Processing Personal Information o.b.o Evolution)

Evolution recognises that third-party operators who process personal information on its behalf present an inherent privacy, information security, and regulatory compliance risk. Accordingly, a structured, risk-based third-party management framework shall be applied in order to comply with, amongst others, sections 19 (Security measures on integrity and confidentiality of

personal information), 20 (Information processed by operator or person acting under authority), 21 (Security measures regarding information processed by operator) and 22 (Notification of security compromises) of POPIA. .

7.1 Due Diligence and Onboarding

7.1.1 All third-party service providers/suppliers that process personal information on behalf of Evolution shall be subjected to formal Third-Party Due Diligence ("DD") prior to onboarding, renewal, or material scope changes. Due diligence shall include, at a minimum:

7.1.2 Assessment of the supplier's POPIA compliance maturity;

7.1.3 Whether they have appointed an Information Officer and is he/she is registered as such with the Information Regulator

7.1.4 Information security, and physical documentation, controls and safeguards;

7.1.5 Data breach management processes;

7.1.6 Sub-processing arrangements, i.e. are sub-operators used, the contractual arrangements for same and, if applicable, was prior written consent obtained from Evolution for such arrangement;

7.1.7 Cross-border data transfer risks (where applicable);

7.1.8 Regulatory licensing and financial soundness (where relevant).

No service provider/supplier, who will be processing personal information, may be engaged without the successful completion of the requisite due diligence process and the execution of an approved Data Processing Agreement (DPA) in addition to a satisfactory Service or Supplier Agreement.

7.2 Third-Party Operator Risk Ranking

7.2.1 7.2.1. All service providers/suppliers processing personal information, i.e. operators, shall be formally risk-ranked using Evolution's approved Third-Party Risk Assessment Matrix. Risk rating shall be based on factors including, but not limited to:

7.2.2 Volume and sensitivity of personal information processed;

Nature and purpose of processing;

Access to special personal information;

7.2.3 Degree of system integration and data access;

7.2.4 Jurisdiction of processing;

7.2.5 History of security or compliance incidents re data privacy breaches or contravention of POPIA.

7.2.6 The assigned risk rating shall determine the applicable review frequency and degree of monitoring intensity, with a strict risk-based approach adopted across all service provider/supplier oversight and/or auditing activities.

7.3 Ongoing Monitoring and Review

7.3.1. Third-party service providers/suppliers shall be subject to ongoing monitoring throughout the lifecycle of the relationship. Monitoring shall include:

Periodic re-assessment in accordance with risk-based review cycles;

Review of continued compliance with POPIA, contractual obligations, and DPAs;
Confirmation of ongoing security and privacy safeguards;
Monitoring of incidents, complaints, or regulatory actions impacting the supplier.

7.3.2. Monitoring responsibility shall be allocated either to:

The designated Relationship Manager, or the compliance officerdepending on operational capacity and risk exposure.

7.4 Training and Accountability

All Evolution employees responsible for the onboarding, contracting, or management of third-party service providers/suppliers (including Relationship Managers and business owners) shall receive mandatory training on:
Third-party POPIA risk;
Due diligence and onboarding procedures;
Use of the risk assessment framework;
Ongoing monitoring requirements; and
Incident reporting obligations.

7.5 Breach Management and Escalation

All third-party agreements, including any DPA, must impose immediate notification obligations in the event of any actual or suspected personal information breach. This requirement is so that Evolution can comply with the requirements of section 22 of POPIA regarding the prescribed timeframe for notifying the Information Regulator of such compromise or breach. Furthermore Evolution shall retain full audit, investigation, and regulatory notification rights as required by POPIA and this must be a specific requirement in any agreement with a third party operator.

7.6 Governance and Oversight

The Third-Party Risk Framework shall be:
Reviewed at least annually, or more frequently where risk requires;
Reported into the Compliance EXCO;
Subject to internal audit or independent assurance where appropriate.

8. Centralised Processing

8.1 In order to:

a. conclude and fulfil contractual terms or obligations to a customer; orb. comply with obligations imposed by law; or

8.1.1 C. to protect or pursue customers', the Group's, or a third party's legitimate interests, including offering solutions that best meet customers' needs;

data subjects' personal information will be processed through centralised functions and systems across companies in the group and may be used for the purposes and/or related purposes, in the manner, and with the appropriate controls as set out in this Policy.

9. Direct Marketing

Direct Marketing will only be conducted as provided for in specific SOP's developed for such channels where direct marketing is conducted.

We will never use any form of electronic communication, including automatic calling machines, facsmile machine,SMSs or email for purposes of direct marketing to any data subject, unless the data subject provided the consent for this purpose.

Where consent is obtained from the data subject, we will ensure that it is voluntary, specific and well informed. We will further ensure that the consent canbe withdrawn by the data subject at any time and will immediately on any request to withdraw consent for direct marketing.

10. Safeguarding Client Information

The Group undertakes to adequately protect personal information.

10.1 The Group will continuously review its security controls and processes to ensure that personal information is secure.

10.2 The following procedures are in place to protect personal information:

10.2.1 The Group Information Officer is Neil Grobbelaar whose details are available below and who is responsible for the compliance with the conditions of the lawful processing of personal information and other provisions of POPI. He is assisted by Deputy Information officers who are all members of the senior management team;

10.2.2 This will be put in place throughout the Group and training on this policy and the POPI Act will be at regular intervals.

10.2.3 Employees are required to sign an employment contract and/or addendum on the use and storage of employee information.

10.2.4 Client information, including archived information, will be dealt with in terms of the relevant Group data security and backup policies.

10.2.5 Suppliers and/or service providers to the Group are required to provide undertakings guaranteeing their commitment to the Protection of Personal Information in accordance with this policy and the SOP's issued in terms hereof; this is an ongoing process that will be evaluated as needed. In so far as any such aforementioned parties meet the definition of Operator We need to sign an Operator Agreement with

such party preferably before they start Processing personal information on our behalf.

10.2.6 The Group will keep a register of all third parties who processes personal information on our behalf.

Actual Or Planned Trans-Border Flows Of Personal Information

10.3 The Group discloses personal information collected to shareholders, funders or third-party service providers, with whom we engage in business or whose services or products we elect to use, including cloud services hosted in international jurisdictions.

10.4 The Group will endeavour to enter into written agreements with or otherwise obtain acceptable undertakings from other parties, to ensure that such parties comply with acceptable confidentiality and privacy requirements. Personal information may also be disclosed where we have a legal duty or a legal right to do so.

11. Data Breach

11.1 Any breach or suspected breach must be dealt with as provided for in the Data Breach Policy and Response Plan as read in conjunction with Disaster Recovery and Business Continuity Policy, if the latter is applicable to the breach or suspected breach..

12. Personal Information – Data Subject Requests and/or Queries

12.1 Clients have the right to access the personal information the Group holds about them.

12.2 Clients also have the right to ask us to update, correct or delete their personal information on reasonable grounds. Once a client objects to the processing of their personal information, we may no longer process said personal information.

12.3 The Group will take all reasonable steps to confirm the client's identity before providing details of their personal information or making changes to their personal information.

12.4 The details of our Information Officer are as follows;

12.4.1 Name: Neil Grobbelaar

12.4.2 Telephone Number: 043 702 4600

12.4.3 Email legalquery@evolution.za.com

12.4.4 Physical Address: 12 Esplanade Road, Quigney, East London

12.4.5 Postal Address: P.O. Box 19610, Tecoma, 5214

12.5 Any request regarding access, correction, deletion or objections in respect of personal information must be dealt with as provided for in the Group Promotion of Access to Information Manual – available at https://www.evolution.za.com/legal-and-compliance/.

Requests will be resolved internally by a specialised team, as provided for in the Complaints Management Policy.

12.6 Data Subjects may also direct any complaints or queries with the information regulator - https://inforegulator.org.za/contact-us/

13. Governance

13.1 Amendments to, or a review of this Policy, will take place on an ad hoc basis or at least once a year. Data Subjects are advised to access our website periodically to keep abreast of any changes. Where material changes affecting clients take place, clients will be notified directly, or changes will be stipulated on our website.