Group Protection of Personal Information Policy

The Kin Group (Pty) Ltd and its subsidiaries | Version V3_2026

Document	Group Protection of Personal Information Policy
Version	V3_2026
Supersedes	Protection of Personal Information Policy V2_2024 (MHA Management Holdings, NHB Administrators and Zazu Life)
Policy Owner	Head of Risk, Legal & Compliance
Responsible Function	Legal & Compliance
Approved by	Head of Risk, Legal & Compliance
Effective Date	Date of signature
Review Frequency	Annually, or earlier upon a material legislative, regulatory or operational change
Next Review Date	12 months after the Effective Date
Related Documents	Group Records Retention and Destruction Policy; Group Privacy Notice; PAIA Manual of each Group Company; Group information security and IT policies; FICA Risk Management and Compliance Programme; Disciplinary Code

APPROVAL AND ADOPTION

By signing below, the Head of Risk, Legal & Compliance approves and adopts this Policy on behalf of The Kin Group (Pty) Ltd and each Group Company to which it applies.

Name and Surname	Stephan Groenewald
Capacity	Head of Risk, Legal & Compliance
Signature	
Date	1 August 2026

1. INTRODUCTION AND PURPOSE

1.1 The Kin Group (Pty) Ltd ("TKG") and its subsidiaries process the personal information of prospective clients, policyholders, insured lives, beneficiaries, claimants, intermediaries, employees, job applicants, suppliers and other stakeholders in the course of rendering financial services, insurance administration, fulfilment and related services.

1.2 This Policy establishes the framework through which each Group Company complies with the Protection of Personal Information Act No. 4 of 2013 ("POPIA"), the Regulations Relating to the Protection of Personal Information, 2018, as amended by Government Notice 6126 of 17 April 2025 ("the Regulations"), and the guidance notes and codes of conduct issued by the Information Regulator ("the Regulator").

1.3 The objectives of this Policy are to:

(a) give effect to the constitutional right to privacy in section 14 of the Constitution of the Republic of South Africa, 1996;

(b) ensure that all processing of personal information by the Group meets the eight conditions for lawful processing set out in Chapter 3 of POPIA;

(c) allocate clear roles, responsibilities and accountability for the protection of personal information across the Group;

(d) enable data subjects to exercise their rights effectively and free of unnecessary obstacles; and

(e) manage the compliance, operational, financial and reputational risk associated with the processing of personal information, including the risk of enforcement notices, administrative fines of up to R10 million, criminal sanctions and civil claims.

2. SCOPE AND APPLICATION

2.1 This Policy applies to TKG and to each of the following subsidiaries (each a "Group Company" and together "the Group"):

Group Company	Registration Number	FSP Number
The Kin Group (Pty) Ltd	2025/438660/07	—
MHA Management Holdings (Pty) Ltd	1996/011241/07	10134
NHB Administrators (Pty) Ltd	2017/513758/07	11314
Zazu Life (Pty) Ltd	2017/516074/07	5070
WISH Fulfilment (Pty) Ltd	2024/098721/07	**Not an FSP**
Fore Financial Services (Pty) Ltd	2024/753986/07	55301

2.2 **WISH Fulfilment (Pty) Ltd is not an authorised financial services provider.** It does not render financial services as defined in the Financial Advisory and Intermediary Services Act No. 37 of 2002, and nothing in this Policy should be read as indicating otherwise.

2.3 Each Group Company is a separate responsible party in respect of the personal information it processes for its own purposes. A Group Company acts as an operator where it processes personal information on behalf of another Group Company, an insurer or another client in terms of a contract or mandate. Nothing in this Policy merges the separate legal personality of the Group Companies or permits personal information to move between them other than in accordance with clause 8.

2.4 This Policy applies to the directors, employees (permanent, fixed-term and temporary), interns, representatives, contractors and consultants of each Group Company, and to operators to the extent provided for in their contracts with the Group.

2.5 This Policy applies to all personal information processed by or on behalf of the Group, in any form or medium, in any filing system and at any location, including remote working environments and cloud services.

2.6 This Policy must be read with the documents listed in the control table above. Where this Policy and another Group policy conflict on the protection of personal information, this Policy prevails unless the other policy imposes a stricter requirement.

3. DEFINITIONS

3.1 Terms defined in POPIA bear the same meaning in this Policy. The following terms are summarised for convenience:

Term	Meaning
Biometrics	A technique of personal identification based on physical, physiological or behavioural characterisation, including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.
Child	A natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him or herself.
Consent	Any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
Data Subject	The natural or existing juristic person to whom personal information relates.
De-identify	To delete any information that identifies the data subject, can be used or manipulated by a reasonably foreseeable method to identify the data subject, or can be linked by a reasonably foreseeable method to other information that identifies the data subject.
Direct Marketing	Approaching a data subject, in person or by mail or electronic communication, for the direct or indirect purpose of promoting or offering to supply any goods or services, or requesting a donation.
Information Officer	In relation to a Group Company, its head as defined in the Promotion of Access to Information Act No. 2 of 2000 ("PAIA"), being its chief executive officer or equivalent, or the person duly authorised by that person.
Deputy Information Officer	A person designated in terms of section 56 of POPIA and section 17 of PAIA to assist the Information Officer.
Operator	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.
Personal Information	Information relating to an identifiable, living, natural person and, where applicable, an identifiable, existing juristic person, including the categories listed in section 1 of POPIA.
Processing	Any operation or activity concerning personal information, whether or not by automatic means, including collection, receipt, recording, organisation, storage, updating, retrieval, use, dissemination, merging, linking, restriction, degradation, erasure and destruction.
Record	Any recorded information, regardless of form or medium, in the possession or under the control of a responsible party, whether or not created by it.
Restriction	To withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy it.

Term	Meaning
Security Compromise	Any situation where there are reasonable grounds to believe that personal information has been accessed or acquired by an unauthorised person.
Special Personal Information	Personal information concerning a data subject's religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information, or criminal behaviour as described in section 26 of POPIA.

4. GOVERNANCE, ROLES AND RESPONSIBILITIES

Boards of Directors

4.1 The board of each Group Company is accountable for that Group Company's compliance with POPIA. A board may delegate responsibilities but not its accountability. Each board must ensure that an Information Officer is in place and registered, that adequate resources are allocated to privacy compliance, and that it receives a report on the state of privacy compliance at least annually and promptly upon any material security compromise.

Information Officer

4.2 The head of each Group Company is its Information Officer by operation of law. The head of each Group Company authorises the Head of Risk, Legal & Compliance in writing to perform the duties of Information Officer for that Group Company.

4.3 The Information Officer of each Group Company must be registered with the Regulator on the Regulator's eServices portal before taking up his or her duties. Registration details must be updated promptly whenever the Information Officer or a Deputy Information Officer changes.

4.4 The Information Officer is responsible for the duties in section 55 of POPIA and regulation 4 of the Regulations, including:

(a) developing, implementing, monitoring and maintaining a compliance framework, of which this Policy forms part;

(b) ensuring that personal information impact assessments are performed in accordance with clause 14;

(c) ensuring that the PAIA manual of each Group Company is developed, monitored, maintained and made available;

(d) ensuring that internal measures and adequate systems are in place to process requests for information or access to information;

(e) ensuring that awareness sessions are conducted on POPIA, the Regulations, codes of conduct and information obtained from the Regulator;

(f) dealing with requests, objections and complaints made by data subjects;

(g) managing the response to, and notification of, security compromises in accordance with clause 11;

(h) maintaining the registers required by this Policy, including the personal information inventory, the operator register, the security compromise register and the request and complaints registers;

(i) approving the personal information protection terms of contracts with operators and other third parties;

(j) co-operating with the Regulator in relation to any investigation, assessment or enforcement process; and

(k) reporting to the boards of the Group Companies in accordance with clause 4.1.

Deputy Information Officers

4.5 The Information Officer may designate one or more Deputy Information Officers in writing. Deputy Information Officers must be registered with the Regulator and assist the Information Officer in the performance of his or her duties. The Information Officer remains responsible for any delegated duty.

Executive and Line Management

4.6 Executives and line managers are the process owners for personal information processed in their areas. They must maintain the entries in the personal information inventory for their areas, implement the controls required by this Policy, apply the retention schedule, ensure that their teams are trained, and report security compromises and data subject requests to the Information Officer without delay.

Information Technology

4.7 The Group's IT function is responsible for implementing and maintaining the technical security safeguards described in clause 11, for performing security due diligence on technology operators and cloud service providers before appointment, for executing deletion and destruction of electronic records in accordance with the Group Records Retention and Destruction Policy, and for detecting, containing and reporting security compromises.

Marketing and Communications

4.8 The marketing function is responsible for ensuring that all direct marketing complies with clause 7, that the Group Privacy Notice and cookie notices on Group websites are current, and that new marketing channels, data sources or outsourced marketing service providers are approved by the Information Officer before use.

People (Human Resources and Learning & Development)

4.9 The People function is responsible for processing employee and job applicant personal information in accordance with this Policy, for including the privacy and confidentiality terms in Annexure A in employment contracts, and for scheduling and recording privacy training in accordance with clause 16.

Employees and Other Persons Acting on Behalf of the Group

4.10 Every employee and person acting on behalf of the Group must:

(a) treat personal information as confidential and process it only to the extent required for his or her duties;

(b) access personal information only through approved Group systems and not save it to personal, unmanaged devices or personal cloud or email accounts;

(c) send personal information outside the Group only through approved and secure channels in accordance with clause 11.3;

(d) not enter personal information into any artificial intelligence tool or other external service that has not been approved by the Group for that purpose;

(e) keep personal information accurate, and verify a data subject's identity before updating or disclosing his or her information;

(f) apply the retention schedule and not create unnecessary copies, filing systems or data sets;

(g) lock screens and devices when unattended, keep passwords confidential, and secure paper records and removable media;

(h) not transfer personal information outside South Africa other than in accordance with clause 10;

(i) immediately report any actual or suspected security compromise to the Information Officer or IT in accordance with clause 11.4; and

(j) complete privacy training as required by clause 16.

5. CONDITIONS FOR LAWFUL PROCESSING

Accountability

5.1 Each Group Company must ensure that the conditions for lawful processing, and all measures that give effect to them, are complied with at the time of determining the purpose and means of processing and during the processing itself (section 8).

Processing Limitation

5.2 Personal information must be processed lawfully and in a reasonable manner that does not infringe the privacy of the data subject, and only if, given the purpose, it is adequate, relevant and not excessive (sections 9 and 10).

5.3 Personal information may only be processed if at least one of the following grounds in section 11(1) applies, and the applicable ground must be recorded for each processing activity in the personal information inventory:

(a) the data subject, or a competent person where the data subject is a child, consents to the processing;

(b) processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party;

(c) processing complies with an obligation imposed by law on the responsible party;

(d) processing protects a legitimate interest of the data subject;

(e) processing is necessary for the proper performance of a public law duty by a public body; or

(f) processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

5.4 Consent is not the default ground. It must be used only where no other ground is available or where POPIA requires it, for example for direct marketing to non-customers and for certain processing of special personal information. Where consent is relied upon, the Group Company bears the burden of proving it and must record when, how and for what purpose it was obtained. A data subject may withdraw consent at any time, without affecting the lawfulness of prior processing.

5.5 A data subject may object, on reasonable grounds and in the prescribed manner (Form 1 of the Regulations), to processing based on paragraphs (d) to (f) of clause 5.3, and may object at any time to processing for direct marketing. Once an objection has

been received, the Group Company may no longer process that personal information on that ground, subject to any other lawful ground that applies.

5.6 Personal information must be collected directly from the data subject, unless an exception in section 12(2) applies, such as where the information is contained in a public record, the data subject has consented to collection from another source, collection from another source is necessary to comply with the law or to conduct legal proceedings, or the data subject is a member of a group scheme and the information is supplied by the employer or scheme in accordance with the scheme's rules.

Purpose Specification

5.7 Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the Group Company, and the data subject must be made aware of that purpose in accordance with clause 5.18 (section 13).

Retention and Restriction of Records

5.8 Records of personal information may not be retained for longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless:

(a) retention is required or authorised by law;

(b) the Group Company reasonably requires the record for lawful purposes related to its functions or activities;

(c) retention is required by a contract between the parties; or

(d) the data subject, or a competent person where the data subject is a child, has consented to the retention.

5.9 Records may be retained for longer periods for historical, statistical or research purposes only where appropriate safeguards are in place against the records being used for any other purpose.

5.10 Where personal information has been used to make a decision about a data subject, the record must be retained for the period required by law or a code of conduct or, if none, for a period that affords the data subject a reasonable opportunity to request access to it.

5.11 As soon as reasonably practicable after a Group Company is no longer authorised to retain a record, it must destroy or delete the record or de-identify it, in a manner that prevents its reconstruction in an intelligible form.

5.12 A Group Company must restrict the processing of personal information instead of destroying it where:

(a) its accuracy is contested by the data subject, for a period enabling the accuracy to be verified;

(b) it is no longer needed for achieving the purpose of processing but must be maintained for purposes of proof;

(c) the processing is unlawful and the data subject opposes destruction or deletion and requests restriction instead; or

(d) the data subject requests that the information be transmitted into another automated processing system.

5.13 Restricted personal information may, with the exception of storage, only be processed for purposes of proof, with the data subject's consent, for the protection of the rights of another person or if required in the public interest. The data subject must be informed before a restriction is lifted.

5.14 Retention periods, triggers, legal holds and approved methods of destruction and de-identification are set out in the Group Records Retention and Destruction Policy and its Retention Schedule, which form part of this Policy's compliance framework.

Further Processing Limitation

5.15 Further processing must be compatible with the purpose of collection, having regard to the relationship between the purposes, the nature of the information, the consequences for the data subject, the manner of collection and any contractual rights and obligations between the parties. Where a proposed further purpose is not compatible and no exception in section 15(3) applies, the data subject's consent must first be obtained.

Information Quality

5.16 Each Group Company must take reasonably practicable steps to ensure that personal information is complete, accurate, not misleading and updated where necessary, having regard to the purpose of processing. The effort applied must be proportionate to the importance of accuracy; beneficiary, banking and contact details used to pay claims or benefits require particular care and independent verification.

Openness

5.17 Each Group Company must maintain the documentation of its processing operations required by section 51 of PAIA, including its PAIA manual.

5.18 When personal information is collected, the Group Company must take reasonably practicable steps to ensure that the data subject is aware of the matters listed in section 18 of POPIA, before collection where collected directly, or as soon as reasonably practicable thereafter where collected from another source. The Group Privacy Notice gives effect to this requirement and must be made available on Group websites, referenced in application forms and policy documentation, and provided on request.

Security Safeguards

5.19 Security safeguards are dealt with in clauses 9 to 11.

Data Subject Participation

5.20 Data subject rights and requests are dealt with in clause 12.

6. SPECIAL PERSONAL INFORMATION AND CHILDREN

6.1 Special personal information may not be processed unless a general authorisation in section 27 or a specific authorisation in sections 28 to 33 of POPIA applies, or the Regulator has granted an exemption.

6.2 In the context of the Group's business, the following authorisations are most commonly relevant and must be recorded in the personal information inventory where relied upon:

(a) health information processed by or for an insurer, or by an administrator acting on its behalf, where necessary for assessing the risk to be insured (where the data subject has not objected), for the performance of an insurance agreement or for the enforcement of contractual rights and obligations (section 32(1)(b));

(b) health information of employees, where necessary to implement laws or collective agreements creating rights dependent on health, or for the reintegration of or support for workers in connection with sickness or work incapacity (section 32(1)(f));

(c) race or ethnic origin where processing is necessary to comply with laws designed to protect or advance persons disadvantaged by unfair discrimination, such as employment equity reporting (section 29(b));

(d) information about criminal behaviour processed for the Group Company's own lawful purposes, including fit and proper assessments and fraud prevention (section 33); and

(e) trade union membership, and any other special personal information not covered above, on the ground of consent or another applicable ground in section 27.

6.3 Health information may only be processed by persons who are subject to a duty of confidentiality, whether by virtue of office, employment, profession or contract. Access must be limited to underwriting, claims and People staff who require it.

6.4 Personal information of children may only be processed where section 35 permits it, including with the prior consent of a competent person or where necessary to establish, exercise or defend a right or obligation in law. Where a child is an insured life, dependant or beneficiary under a policy, the policyholder acting as a competent person and the performance of the policy will ordinarily provide the basis for processing. Children's personal information may never be used for direct marketing.

7. DIRECT MARKETING

7.1 Direct marketing by means of unsolicited electronic communications, including email, SMS, instant messaging, automated calling and telephone calls as interpreted in the Regulator's Guidance Note on Direct Marketing, is permitted only in accordance with section 69 of POPIA and regulation 6 of the Regulations.

7.2 A non-customer may only be approached with direct marketing if he or she has given consent in the manner prescribed by regulation 6, as amended. A non-customer may be approached once only to request consent, and may not be approached if consent has previously been withheld.

7.3 An existing customer may be approached with direct marketing only where his or her contact details were obtained in the context of the sale of a product or service, the marketing relates to the Group Company's own similar products or services, and the customer was given a reasonable opportunity to object, free of charge, when the details were collected and on each subsequent communication.

7.4 An opt-out mechanism, a pre-ticked box or silence does not constitute consent. Consent records must be retained in accordance with the Retention Schedule.

7.5 Every direct marketing communication must identify the sender and contain an address or other contact details to which the recipient may send a request to stop such communications.

7.6 Each Group Company is a separate responsible party for direct marketing purposes. A Group Company may not use personal information collected by another Group

Company to market its own products or services unless the requirements of clause 7.2 or 7.3 are met in respect of the marketing Group Company.

7.7 The Group maintains a single suppression list. An objection or opt-out received by any Group Company must be recorded on that list and honoured across the Group without delay.

7.8 Outsourced call centres and marketing service providers are operators and may only be appointed in accordance with clause 9 and with the prior approval of the Information Officer.

8. INTRA-GROUP SHARING OF PERSONAL INFORMATION

8.1 Personal information may be shared between Group Companies only where the receiving Group Company has a lawful ground for the processing, the processing is compatible with the purpose of collection, and data subjects have been informed of the sharing in the Group Privacy Notice or otherwise.

8.2 Where a Group Company provides shared services to another Group Company, including administration, IT, finance and People services, and in doing so processes personal information on its behalf, it acts as an operator. An intra-group data processing agreement complying with sections 20 and 21 of POPIA must be in place for such arrangements.

8.3 Shared systems must apply role-based access controls that segregate personal information by Group Company and limit access to persons who require it for their duties.

8.4 The Information Officer must maintain a register of intra-group data flows, recording the Group Companies involved, the categories of personal information, the purpose, the lawful ground and the governing agreement.

9. OPERATORS AND THIRD PARTIES

9.1 Before appointing an operator, the responsible Group Company must perform due diligence proportionate to the risk, covering at least the operator's security safeguards, the location of processing and storage, the use of sub-operators and its incident history.

9.2 Every operator must be appointed in terms of a written contract that contains, at a minimum, the terms set out in Annexure B, including the obligations to process personal information only with the knowledge or authorisation of the Group Company, to treat it as confidential, to maintain the security measures in section 19, and to notify the Group

Company immediately where there are reasonable grounds to believe that a security compromise has occurred.

9.3 Where a Group Company acts as operator for an insurer or other client, it must process personal information only in accordance with that client's mandate, comply with the contractual privacy obligations owed to that client, and notify that client immediately of any security compromise.

9.4 The Information Officer must maintain a register of operators, recording the services provided, the categories of personal information, the processing locations and the contract governing the appointment.

10. TRANSBORDER INFORMATION FLOWS

10.1 Personal information may only be transferred to a third party in a foreign country where section 72 of POPIA permits it, namely where:

(a) the recipient is subject to a law, binding corporate rules or a binding agreement that provides an adequate level of protection substantially similar to the conditions for lawful processing, including provisions on onward transfer;

(b) the data subject consents to the transfer;

(c) the transfer is necessary for the performance of a contract between the data subject and the Group Company, or for pre-contractual measures taken in response to the data subject's request;

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the Group Company and a third party; or

(e) the transfer is for the benefit of the data subject, it is not reasonably practicable to obtain consent and, if it were, the data subject would be likely to give it.

10.2 The use of cloud or hosted services located outside South Africa constitutes a transborder transfer. Each such service must be assessed and documented, must be governed by contractual terms that satisfy clause 10.1(a), and must be approved by the Information Officer before personal information is migrated to it.

10.3 The Information Officer must determine whether prior authorisation from the Regulator is required under section 57 of POPIA before any new processing involving the transfer of special personal information or children's personal information to a country without an adequate level of protection, the linking of unique identifiers with information

processed by other responsible parties, or the processing of information on criminal behaviour on behalf of third parties.

11. SECURITY SAFEGUARDS AND SECURITY COMPROMISES

11.1 Each Group Company must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures. It must identify reasonably foreseeable internal and external risks, establish and maintain appropriate safeguards, regularly verify that the safeguards are effectively implemented, and update them in response to new risks, having due regard to generally accepted information security practices (section 19).

11.2 The Group's safeguards include, as a minimum: role-based access control and multi-factor authentication; encryption of personal information in transit and, for portable devices and sensitive repositories, at rest; endpoint protection, patch management and firewalls; logging and monitoring of access to systems holding personal information; regular, tested and protected backups; physical access controls; secure disposal of records and media; and business continuity arrangements.

11.3 Personal information may be sent outside the Group only through approved secure channels, such as encrypted email, secure file transfer or approved client portals. Special personal information and bulk personal information may never be sent by unencrypted email. Where password-protected files are used, the password must be communicated through a separate channel.

11.4 Security compromises must be managed as follows:

(a) any employee or person acting on behalf of the Group who becomes aware of or suspects a security compromise must report it immediately, and in any event within 24 hours of becoming aware of it, to the Information Officer or IT;

(b) IT, under the direction of the Information Officer, must take immediate steps to contain the compromise, preserve evidence and determine its scope;

(c) where there are reasonable grounds to believe that personal information has been accessed or acquired by an unauthorised person, the Group Company must notify the Regulator and, unless the identity of the data subjects cannot be established, the affected data subjects, as soon as reasonably possible after discovery, taking into account the legitimate needs of law enforcement and the measures reasonably necessary to determine the scope of the compromise and restore the integrity of the information system (section 22);

(d) notification to the Regulator must be made in the prescribed form through the Regulator's eServices portal;

(e) notification to data subjects must be in writing, by mail, email, publication on the Group Company's website, publication in the news media or as the Regulator directs, and must contain sufficient information to allow them to take protective measures, including a description of the possible consequences, the measures taken or intended to be taken, recommended measures for the data subject and, if known, the identity of the unauthorised person;

(f) where a Group Company acts as operator, it must notify the responsible party immediately;

(g) the Information Officer must inform the board of the affected Group Company and, where applicable, assess and attend to any notification required to the Financial Sector Conduct Authority or the Prudential Authority under applicable cybersecurity and incident reporting requirements; and

(h) every security compromise must be recorded in the security compromise register and followed by a post-incident review of root cause and remedial actions.

12. DATA SUBJECT RIGHTS AND REQUESTS

12.1 The Group gives effect to the rights of data subjects in section 5 of POPIA, including the right to be notified of collection and of security compromises, to access personal information, to request correction, destruction or deletion, to object to processing and to direct marketing, not to be subject to certain automated decisions, to submit a complaint to the Regulator, and to institute civil proceedings.

12.2 **Access.** A data subject may request a Group Company to confirm, free of charge, whether it holds personal information about him or her, and may request the record or a description of the information, including the identity of third parties who have had access to it. Requests for a record are dealt with in accordance with PAIA and the Group Company's PAIA manual, including the prescribed forms, fees, time periods and grounds for refusal. The requester's identity must be verified before any information is disclosed.

12.3 **Correction, destruction and deletion.** A data subject may request, in the prescribed manner (Form 2 of the Regulations), that personal information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully be corrected or deleted, or that a record the Group Company is no longer authorised to

retain be destroyed or deleted. The Group Company must, as soon as reasonably practicable, comply with the request or provide credible evidence in support of the information, and must notify the data subject of the action taken. Where the change affects decisions about the data subject, the Group Company must, where reasonably practicable, inform third parties to whom the information was disclosed.

12.4 **Objection.** Objections must be submitted in the prescribed manner (Form 1 of the Regulations) and dealt with in accordance with clause 5.5.

12.5 Prescribed forms are available from the Information Officer and on Group websites. The Group will provide reasonable assistance, free of charge, to a data subject who requires help to complete a prescribed form.

12.6 Any employee who receives a data subject request must forward it to the Information Officer within one working day. The Information Officer must record every request and its outcome in the request register.

13. AUTOMATED DECISION-MAKING

13.1 A data subject may not be subjected to a decision that results in legal consequences for him or her, or affects him or her to a substantial degree, which is based solely on automated processing intended to provide a profile of certain aspects of his or her personality or behaviour, unless section 71(2) applies.

13.2 Where automated underwriting, claims assessment, fraud scoring or similar models produce such decisions, the Group Company must ensure that the decision is taken in connection with the conclusion or execution of a contract and either the data subject's request has been met or appropriate measures protect his or her legitimate interests. Those measures must include an opportunity to make representations about the decision, sufficient information about the underlying logic of the processing, and human review on request.

13.3 All such models must be recorded in the personal information inventory and subjected to a personal information impact assessment before deployment.

14. PERSONAL INFORMATION IMPACT ASSESSMENTS AND INVENTORY

14.1 A personal information impact assessment must be performed, and approved by the Information Officer, before the Group introduces or materially changes any product, system, process, channel or operator that involves personal information, and in particular before any new processing of special personal information or children's

personal information, any new transborder transfer, any automated decision-making or any use of artificial intelligence tools involving personal information.

14.2 Each Group Company must maintain a personal information inventory recording, for each processing activity, the categories of data subjects and personal information, the purpose, the lawful ground (and the authorisation for any special personal information), the source, the recipients and operators, any transborder transfers, the applicable retention category and the key security controls. The inventory must be reviewed at least annually.

15. MONITORING, CALL RECORDING AND CCTV

15.1 Telephone calls may be recorded for purposes of quality assurance, record-keeping, regulatory compliance, fraud prevention and dispute resolution. Callers must be informed at the start of a call that it is being recorded, and recordings must be retained and destroyed in accordance with the Retention Schedule.

15.2 Monitoring of Group communication systems and premises, including CCTV, is conducted only for legitimate business purposes, in accordance with the Regulation of Interception of Communications and Provision of Communication-Related Information Act No. 70 of 2002 and Group IT policies, and with appropriate notice to employees and visitors.

16. TRAINING AND AWARENESS

16.1 All new employees must complete privacy training within their first month of employment. All employees must complete refresher training at least annually, and employees in high-risk roles, including underwriting, claims, call centre, marketing, IT and People, must complete role-specific training. Training completion is recorded by the Learning & Development function and reported to the Information Officer.

17. MONITORING AND ASSURANCE

17.1 The Information Officer must ensure that a POPIA compliance assessment of each Group Company is performed at least annually. The assessment must review the personal information inventory and data flows, verify that purposes and lawful grounds remain valid and processing remains adequately limited, test compliance with this Policy and the Retention Schedule, assess the effectiveness of security safeguards and operator controls, and track remediation of previous findings.

17.2 In performing the assessment, the Information Officer has direct access to, and the support of, line management and the boards of the Group Companies. The results are

reported to the boards in accordance with clause 4.1 and may be relied upon in the Group's combined assurance processes.

18. COMPLAINTS

18.1 Data subjects may submit complaints about the processing of their personal information to the Information Officer in writing. The Group will deal with complaints as follows:

(a) any person other than the Information Officer who receives a complaint must ensure that its full details reach the Information Officer within one working day;

(b) the Information Officer will acknowledge receipt in writing within two working days;

(c) the Information Officer will consider the complaint fairly and in accordance with POPIA, determine whether it discloses a security compromise or a systemic issue, and act in accordance with clause 11 where it does;

(d) the Information Officer will respond to the complainant within seven working days of receipt with a proposed resolution and reasons, or will inform the complainant of the reasons for any delay and the expected response date; and

(e) the Information Officer will inform the complainant of his or her right to submit a complaint to the Regulator if dissatisfied with the outcome.

18.2 Complaints are recorded in the complaints register and analysed periodically to identify and address root causes.

19. NON-COMPLIANCE

19.1 A breach of this Policy may constitute misconduct and will be dealt with in accordance with the Group's Disciplinary Code. Minor or inadvertent breaches may be addressed through additional training. Gross negligence or the wilful mishandling of personal information is serious misconduct that may justify dismissal.

19.2 Following an investigation, the Group may also refer a matter to law enforcement, recover losses, or exercise contractual remedies against an operator or contractor. Employees should be aware that certain conduct, including breaches of confidentiality and the unlawful handling of account numbers, constitutes an offence under Chapter 11 of POPIA.

20. REVIEW

20.1 This Policy must be reviewed annually by the Policy Owner, or earlier where required by a material legislative, regulatory or operational change. The Information Officer may update operational procedures, registers and the templates in the Annexures without re-approval of this Policy, provided that they remain consistent with it.

ANNEXURE A

Employee Privacy and Confidentiality Clause (for inclusion in employment contracts)

---

1. Definitions. In this clause, "POPIA" means the Protection of Personal Information Act No. 4 of 2013, and "Personal Information" and "Special Personal Information" bear the meanings given in POPIA.

2. Processing of the Employee's Personal Information. The Employer will process the Employee's Personal Information in accordance with POPIA and the Group Protection of Personal Information Policy for purposes connected with the employment relationship, including recruitment, administration of remuneration and benefits, performance and conduct management, training, health and safety, fit and proper and other regulatory requirements, employment equity, and compliance with tax, labour and financial sector laws. The Employer relies on the performance of the employment contract, compliance with obligations imposed by law and its legitimate interests as the grounds for such processing, and on consent only where the law requires it.

3. Special Personal Information. The Employer may process the Employee's health information where necessary for the administration of sick leave, incapacity, benefits and occupational health and safety; race and related information where necessary for employment equity compliance; and criminal, credit and qualification information where necessary for fit and proper, vetting and fraud prevention purposes, in each case as permitted by POPIA.

4. Disclosure and Transfer. The Employer may disclose the Employee's Personal Information to other companies in The Kin Group, to service providers acting as operators (such as payroll, benefits, screening and IT providers), to retirement funds and insurers, and to regulators and authorities where required by law. Personal Information may be transferred outside South Africa, including to cloud service providers, only in accordance with section 72 of POPIA.

5. Monitoring. The Employee acknowledges that the Employer's communication systems, devices and premises are monitored in accordance with the Employer's IT policies and applicable law.

6. Rights. The Employee may request access to, correction or deletion of, and object to the processing of, his or her Personal Information in accordance with POPIA and the Employer's PAIA manual, and may complain to the Employer's Information Officer or to the Information Regulator.

7. Retention. The Employee's Personal Information will be retained in accordance with the Group Records Retention and Destruction Policy.

8. **Confidentiality of Others' Personal Information.** The Employee will have access to the Personal Information of clients, policyholders, suppliers and colleagues. The Employee must treat such information as strictly confidential, process it only as required for his or her duties and in accordance with Group policies, not disclose it to any person within or outside the Group except as required for those duties or by law, and report any actual or suspected security compromise immediately. These obligations survive the termination of employment. A breach of this clause may result in disciplinary action, including dismissal, and may constitute an offence under POPIA.

9. **Accuracy.** The Employee must inform the Employer promptly of any change to his or her Personal Information.

ANNEXURE B

Operator Data Processing Clause (minimum terms for contracts with operators)

1. Definitions. "POPIA" means the Protection of Personal Information Act No. 4 of 2013 and its Regulations. "Personal Information", "Processing", "Operator", "Responsible Party" and "Security Compromise" bear the meanings given in POPIA. The Group Company is the Responsible Party and the Service Provider is the Operator.

2. Instructions. The Service Provider shall process Personal Information only with the knowledge or authorisation of the Group Company, only for the purpose of providing the services under this agreement, and in accordance with the Group Company's documented instructions. It shall not process Personal Information for its own purposes.

3. Confidentiality. The Service Provider shall treat Personal Information as confidential, shall not disclose it unless required by law or in the course of the proper performance of its duties, and shall ensure that all persons authorised to process it are bound by confidentiality obligations.

4. Security. The Service Provider shall establish and maintain the security measures referred to in section 19 of POPIA, having regard to generally accepted information security practices and any specific requirements of the Group Company, and shall provide evidence of these measures on request.

5. Security Compromises. The Service Provider shall notify the Group Company immediately, and in any event within 24 hours, where there are reasonable grounds to believe that Personal Information has been accessed or acquired by an unauthorised person, and shall provide all information and co-operation reasonably required for the Group Company to meet its obligations under section 22 of POPIA. The Service Provider shall not notify data subjects or the Information Regulator without the Group Company's prior written consent, unless required by law.

6. Sub-Operators. The Service Provider shall not appoint a sub-operator without the Group Company's prior written consent and shall impose on any approved sub-operator obligations no less protective than those in this clause. The Service Provider remains liable for the acts and omissions of its sub-operators.

7. Transborder Transfers. The Service Provider shall not process or store Personal Information outside South Africa, or permit access to it from outside South Africa, without the Group Company's prior written consent and then only in compliance with section 72 of POPIA.

8. Assistance. The Service Provider shall promptly refer to the Group Company any request, objection or complaint from a data subject or the Information Regulator, and shall assist the Group Company to respond to it and to perform impact assessments.

9. Retention, Return and Destruction. The Service Provider shall retain Personal Information only for as long as required to provide the services or as instructed by the Group Company. On termination, or earlier on request, it shall return or securely destroy all Personal Information, including copies, and provide a written certificate of destruction.

10. Audit. The Group Company, its auditors and regulators may, on reasonable notice, audit the Service Provider's compliance with this clause.

11. Indemnity. The Service Provider indemnifies the Group Company against all losses, fines, claims and costs arising from any breach of this clause by the Service Provider or its sub-operators.