

# UAP OLD MUTUAL PRIVACY POLICY – LEVEL II

**Policy Number**

P11.03

**Contact**

UAP OM Group Chief Operations Officer

**Version/Date**

**1 November 2020**

We regularly review our Privacy Policy and you will find the most recently updated Policy on our company website, [www.uapoldmutual.com](http://www.uapoldmutual.com). This version was last updated on 1 November 2020.

## 1. What is the purpose of this Policy?

Welcome to the UAP Old Mutual Group's Data Privacy Policy. The UAP Old Mutual Group respects your privacy and is committed to protecting your personal data. This Privacy Policy will inform you as to how the UAP Old Mutual Group collects, uses, discloses, transfers and stores your personal data when you interact with us and tells you about your privacy rights and how the law protects you. Since we want to empower you to make the best decisions about your privacy and personal data, we have made this Privacy Policy as clear and transparent as possible to let you know how the law protects you. It is therefore important that you read this Privacy Policy and understand what we intend to do with your personal data.

## 2. Who does the policy apply to?

The UAP Old Mutual Group comprises different legal entities which provide various products or services including insurance, banking, asset management and investment solutions. The following are the legal entities in Kenya that form part of the UAP Old Mutual Group and are responsible for your personal data in terms of this Privacy Policy:

No.	Entity	Contact Details
1.	UAP Holdings Plc	UAP Old Mutual Tower, Upper Hill Road P.O. Box 43013 - 00100, Nairobi, Kenya Tel: + 254 20 2850000 Mobile: + 254 711 065 000 Fax: + 254 20 2719 030 E-mail: <a href="mailto:uapholdings@uap-group.com">uapholdings@uap-group.com</a> Website: <a href="http://www.uap-group.com">www.uap-group.com</a>
2.	UAP Insurance Company Limited	UAP Old Mutual Tower, Upper Hill Road P.O. Box 43013 - 00100, Nairobi, KENYA Tel: + 254 20 2850 000 Mobile: + 254 711 065 000 Fax: + 254 20 2719 030 E-mail: <a href="mailto:uapinsurance@uap-group.com">uapinsurance@uap-group.com</a>
3.	Old Mutual Life Assurance Company Limited	UAP Old Mutual Tower, Upper Hill Road PO Box 30059 - 00100, Nairobi, Kenya Tel +254 (20) 2829 000 / 2728 881 Email: <a href="mailto:clientservices@oldmutualkenya.com">clientservices@oldmutualkenya.com</a>
4.	Old Mutual Investment Group Limited	UAP Old Mutual Tower, Upper Hill Road P.O. Box 11589, GPO 00400 Nairobi, Kenya Tel +254 (20) 282 9800, 272 8881 Email: <a href="mailto:omigclientservice@oldmutualkenya.com">omigclientservice@oldmutualkenya.com</a>
5.	Old Mutual Securities Limited	UAP Old Mutual Tower, Upper Hill Road P.O. Box 50338-00200 Nairobi, Kenya Tel +254 720 909 091, +254 (20) 224 1408, +254 73100 206 Email: <a href="mailto:omsclientservice@oldmutualkenya.com">omsclientservice@oldmutualkenya.com</a>
6.	UAP Life Assurance Limited	UAP Old Mutual Tower, Upper Hill Road P.O. Box 23842 – 00100, Nairobi, Kenya Tel: +254 20 2850 300 Mobile: +254 711 065 300

		Fax: + 254 20 2719 030 E-mail: <a href="mailto:life@uap-group.com">life@uap-group.com</a>
7.	Faulu Microfinance Bank Limited	<b>Head Office Address:</b> Ngong lane, off Ngong Road P.O.Box 60240-00200 Nairobi, Kenya <b>Telephone:</b> +254 711 074 000 or +254 711 074 074 <b>Email:</b> <a href="mailto:info@faulukenya.com">info@faulukenya.com</a>
8.	Old Mutual Holdings Limited	UAP Old Mutual Tower, Upper Hill Road PO Box 30059, GPO 00100, Nairobi, Kenya Tel +254 (20) 2211 87/8

This Privacy Policy is issued on behalf of the UAP Old Mutual Group so when we mention “**UAP Old Mutual Group**”, “**we**”, “**us**” or “**our**” in this Privacy Policy, we are referring to the relevant company in the UAP Old Mutual Group set out above responsible for processing your personal data when you purchase a product or service from us.

### 3. What risks are managed by this policy?

Regulatory Compliance risk is defined as the risk of breaching laws, regulations or regulatory directives, resulting in possible fines, regulatory sanctions, reputational damage and/or financial loss. For the purposes of this Policy the following definitions are used:

- 3.1 Privacy Risk: The risk of a Data Breach or the use of Personal Information in an inappropriate manner, contrary to applicable legal and/or regulatory obligations.
- 3.2 Data Breach: The loss or theft of Personal Information or unauthorised access to Personal Information.
- 3.3 Employee: The term includes direct employees, agents, other permanent staff such as fixed term or independent contractors, as well as any temporary staff including temporary contractors or service providers that are in service of the UAP Old Mutual Group.
- 3.4 Notice: A declaration or notification by a legal entity of the UAP Old Mutual Group setting out the role of the entity, what will be done with the Personal Information and with whom it will be shared.
- 3.5 Personal Information: Personal data or information related to an identifiable living individual.

## 4. What risk appetite statements apply to this policy?

We have **Low** preference for any information security breach in which significant amounts of confidential data affecting our clients, and/or proprietary information has been compromised that can result in regulatory notification, reputational damage, customer impact or financial impact, reporting impact or legal impact.

We have a **Low** or limited appetite for Regulatory Compliance risks. We are committed to complying with regulatory requirements in both the spirit and the letter of the law. We acknowledge that noncompliance may occur from time to time, but have **Zero** appetite for deliberate non-compliance.

Where Regulatory Compliance risks arise we will take appropriate steps to mitigate these.

## 5. What are the minimum mandatory requirements of this policy?

The Group has put in place the following policies and processes to ensure that the personal information and sensitive personal information is collected, stored and used in line with the requirements of the applicable data protection laws:

### 5.1 COLLECTION

Personal data means any information relating to an identified or identifiable natural person. The personal data that we collect will depend on the context of our relationship with you. We may collect, use, store and transfer different kinds of personal data about you or persons connected to you which we have grouped together as follows:

- identification information such as name, date and place of birth, national identity card number, passport number, Kenya Revenue Authority personal identification number (PIN), photo, marital status, title, nationality, gender and specimen signature.
- contact information such as email address, postal address, physical address, residential address and telephone number.
- financial information such as bank account details, payment card details, mobile money statements, income, credit history, credit worthiness, bank statements, details about payments to or from you and other details of products and services you have purchased from us.
- information relevant to your insurance policy or relevant to your claim or your involvement in the matter giving rise to a claim.
- Information about the nature of your business and commercial assets.
- employment information such as the name of the employer, position in the organization and office address.
- children's personal data such as the name, date of birth and gender.
- sensitive personal information such as marital status, property details, health status and family details (such as next of kin and beneficiaries).
- marketing and communications information including your preferences in receiving marketing information from us and communication from us.

- online data whenever you use our products and services through our website, mobile applications such as cookies, login data, IP address (your computer's internet address), browser type and version, ISP or operating system, domain name, access time, page views, location data, how you frequently use our online insurance, banking and other services, our mobile applications or visit our website.
- profile data such as your username and password, purchases or orders made by you, your interests, preferences, feedback and survey responses.

If we need information about other people connected to you, we may request you to provide the information in relation to those people. If you are providing information about another person, we expect you to ensure that they know you are doing so and are content with their information being provided to us. It might be helpful to show them this Privacy Policy and if they have any concerns, please contact us on the same.

The list below shows you the various ways we may collect your personal information (please note that this list is not exhaustive):

**We may collect personal data directly from you**

In most instances, we collect personal data directly from you when you fill in forms or communicate with us through our contact details. This includes personal data you provide when you:

- apply for our products or services;
- make enquiries;
- create an account on our website;
- register for our products offered through mobile and online platforms;
- request marketing information to be sent to you;
- give us feedback or contact us;
- provide goods or services to us as a supplier or contractor; or
- interact with our website. We collect this personal data by using cookies and similar technologies. You can find out more about this in our cookies and website policy;

**We may collect your personal data from a number of third parties or publicly available sources**

In some instances, we will receive your personal data from various third parties or publicly available sources including:

- identity and contact data from the Government of Kenya's e-citizen and Integrated Population Registration Services platforms;
- identity and contact data from publicly available sources such as the Companies Registry and the Business Registration Service
- contact, financial and transaction data from land registries, industry databases such as credit reference agencies, fraud prevention agencies and providers of technical, payment and delivery services;
- medical professionals and hospitals;

- social media. If you are a potential candidate for employment with UAP Old Mutual Group, we may have received your personal data from third parties such as recruiters or external websites.
- directly from an individual or employer (or your employer's service provider) who has a policy with us under which you are insured.
- directly from an employer which funds a cover that we administer where you are a beneficiary.
- directly from a person who is making a claim or application and they include information about you which is related to their claim or application.
- from your family members when they make enquiries about purchasing a product for you or including you on their insurance, when you ask them to make a claim on your behalf, or where you may be incapacitated or otherwise unable to provide information yourself when we need it;
- your insurance broker if you have one.
- third parties who assist us in checking that claims are eligible for payment.

## 5.2 CHOICE AND CONSENT

Where we need to collect personal data by law, or under the terms of a contract we have with you, and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with an insurance policy or to provide you with banking services). In this case, we may have to cancel a product or service you have with us but we will notify you if this is the case within reasonable time.

You have the right to withdraw your consent to our processing of your personal data at any time but please note, that your withdrawal will not affect the lawfulness of our processing which was based on prior consent before your withdrawal or which is based on other legal basis for processing your personal data. Please however note that in some instances, we will not be able to provide our products and services if you withdraw your consent.

## 5.3 USE OF PERSONAL DATA

We will only use your personal data when the law allows us. Most commonly, we will use your personal data in the following circumstances:

- where we need to perform the contract we are about to enter into or have entered into with you.
- to assess whether you are eligible for our products and services.
- where you consent to our use of your personal data.
- where we need to comply with or fulfil legal or regulatory obligations and protecting ourselves and our clients against fraud.
- where we need to protect your vital interests and the vital interests of third parties (for example when paying out sums to beneficiaries under your policies).

- where it is necessary for our legitimate interests (or those of a third party) such as maintaining our records, developing, assessing and improving our products and services, risk evaluation, underwriting, managing arrangements with reinsurers, managing claims, improving our customer administration and engagement as well as complying with our Know Your Customers (KYC) requirements.
- to establish, exercise or defend our legal rights such as when we are faced with any legal claim or where we want to pursue any legal claims.
- to advertise and market to you our latest products and services (please note that if you do not want to receive our marketing information you may opt-out anytime by contacting us at any time).
- to send you important notices such as changes to our terms, conditions and policies or unusual activity with respect to any of your accounts with us.
- if you apply for an employment position at UAP Old Mutual Group or we note that you are a potential candidate for employment, we may use your personal data in evaluating your candidacy and to contact you about the employment opportunity.
- where we receive your personal data from third parties, we may use it to validate the information you have provided to us or for fraud prevention purposes.
- to enable you use the services available through our website and mobile and online applications including registering you for our services and verifying your identity and authority to use our services.
- to address fraud or safety concerns, or to investigate complaints or suspected fraud or illegality.
- to monitor and analyse the use of our products and services for system administration, operation, testing and support purposes.
- to cooperate with, respond to requests from, and to report transactions and/or other activity to, government, tax or regulatory bodies, financial markets, brokers or other intermediaries or counterparties, courts or other third parties.
- to conduct compliance activities such as audit and reporting, assessing and managing risk, maintenance of accounting and tax records, fraud and anti-money laundering (AML) prevention and measures relating to sanctions and anti-terrorism laws and regulations and fighting crime. This includes know your customer (KYC) screening (which involves identity checks and verifying address and contact details), politically exposed persons screening (which involves screening client records against internal and external databases to establish connections to 'politically exposed persons' (PEPs) as part of client due diligence and onboarding) and sanctions screening (which involves the screening of clients and their representatives against published sanctions lists).
- to record and/or monitor telephone conversations so as to maintain service quality and security, for staff training and fraud monitoring and to deal with complaints, disputes and potential and/or actual criminal activity. To the extent permitted by law, these recordings are our sole property.

#### 5.4 RETENTION AND DISPOSAL

We will only retain your personal data for as long as may be reasonably necessary to fulfil the purpose we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting information.

We may retain your personal data for a longer period if the retention is:

- required or authorised by law.
- reasonably necessary for a lawful purpose.
- authorised or consented by you.
- Is necessary for purposes of responding to a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.
- for historical, statistical, journalistic, literature and art or research purposes.

#### 5.5 ACCESS

It is important that the personal data we hold about you is accurate and the most recent. We encourage you to keep us informed in case of any changes of your personal data during your relationship with us.

#### 5.6 THIRD PARTY DISCLOSURE

Subject to your rights and the applicable laws, we may share your personal data with the third parties set out below:

- entities comprising the UAP Old Mutual Group or their affiliates.
- public authorities or governments when required by law, public interest, national security, regulation, legal process or enforceable governmental request.
- our third-party service providers who help us manage our products and services including those service providers who maintain our IT and office systems and provide marketing and advertising services.
- to service providers that provide application processing, fraud monitoring, call center and/or other customer services, hosting services and other technology and business process outsourcing services.
- persons or entities that you explicitly request us to transfer your personal data to them.
- your relatives, guardians or persons acting on your behalf where you are incapacitated or for the purposes of paying out claims to your beneficiaries.
- financial advisers, business partners and third party administrators who help us manage our products and services.
- banks or financial institutions within the country and outside the country where you either transfer or receive payments from the said banks or financial institutions.
- insurers, reinsurers and brokers who help us manage and underwrite our products and provide us with reinsurance and insurance services.
- our professional advisers such as auditors, tax advisers, insurers, reinsurers, medical agencies, legal advisers who act on our or your behalf, or who represent another third party.
- loss adjusters and claims experts who help us handle claims.



- medical institutions and professionals where we may require to access your health records and assessments for the purpose of arranging or facilitating your claim.
- third parties connected with the sale, transfer or disposal of our business.
- to counterparty banks, payment infrastructure providers and other persons from whom we receive, or to whom we make, payments on our clients' behalf.
- debt collection agencies, credit reference agencies, fraud detection agencies and other agencies that we will contract to provide services to us.

### 5.7 DATA SECURITY

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

### 5.8 CROSS BORDER TRANSFER OF PERSONAL DATA

Where we will make a transfer of your personal data outside Kenya, we will ensure that adequate steps are taken to protect your privacy rights and your personal data. These include:

- Providing proof to the Data Protection Commissioner of the appropriate safeguards taken to protect your personal data.
- Where your personal data is transferred to our affiliates located outside the country, we have entered into agreements governing transfers of personal data with our affiliates to ensure that your personal data receives an adequate and consistent level of protection.
- We will only transfer your sensitive personal data outside Kenya where we have obtained your consent and on confirmation of appropriate safeguards. Such safeguards may include placing the third party to whom the personal data is transferred under contractual commitments to protect the personal data as well as transferring the personal data to jurisdictions with commensurate levels of protection to ours.

### 5.9 YOUR LEGAL RIGHTS

---

You have the right to:

- be informed of the use to which your personal data is to be put as we have endeavoured to outline in this Privacy Policy;
- request access to your personal data that we hold about you;
- object to the processing of all or part of your personal data;
- request correction of inaccurate, false or misleading data that we hold about you; and
- request deletion of false or misleading data that we hold about you.

## 6. How to reach us

We have appointed a data protection officer who is responsible for overseeing questions in relation to this Privacy Policy.

If you have any concerns about the use of your personal data, questions about this Privacy Policy including any requests to exercise your legal rights under the law, please contact us using the details set out below:

Email address: [dataprivacy@uapoldmutual.com](mailto:dataprivacy@uapoldmutual.com)  
Postal address: P.O. Box 43013 – 00100, Nairobi  
Physical address: UAP Old Mutual Tower, Upper Hill Nairobi  
Telephone number: +254 20 2850000

We will respond to your questions or concerns within [seven (7) days] of receipt of the query.