



PRIVACY POLICY

ALCOFUND publishes, operates and markets the MiQo financial services platform (the "Platform") accessible at <https://www.mymiqo.com>, which allows you to:

- Recharge an account opened on the platform;
- Receive payment;
- To transfer money;
- Buy prepaid cards;
- Generate a virtual card
- Buy phone credit;
- Create and participate in savings pools;
- Pay bills online or at a local merchant;
- Buy communication credit;
- Access instant nano-loans;
- make savings;
- Access financial education articles and videos.

ALCOFUND acts within the meaning of the Cameroonian, CEMAC ZONE and European regulations on data protection, applicable, as data controller ("Data controller") in that we are the only ones to define the purpose and means of processing. data collected from you.

It is therefore our responsibility, and under our sole responsibility, to comply with the provisions of the regulations applicable in Cameroon and in particular with regard to obtaining your consent prior to any processing of your personal data. We apply to all data processing carried out under our responsibility, the principles of lawfulness, fairness, transparency, limitation of purposes, minimization of data, accuracy, integrity of confidentiality and limitation in the duration of data retention. about you.

The transparency and protection of your privacy and your personal data, particularly in terms of security, is one of our fundamental missions. The purpose of this privacy policy is to inform you about how we collect, use, store or transfer your personal data.





I. COLLECTION AND USE OF YOUR PERSONAL DATA

WHAT IS PERSONAL DATA ?

The term "personal data" means any information relating to an identified or identifiable natural person, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural identity, or social (article 2 of the Consumer Protection Harmonization Directive within CEMAC).

In this sense, personal data can be considered as full name, social security number, national identity card number, passport number, account number, date and place of birth, physical address and e-mail, telephone number, bank card number, biometric data such as fingerprints and DNA, etc.

YOUR CONSENT TO THE TREATMENT IS ALWAYS REQUIRED

We ensure, before any collection, that your consent is explicit and free, for this purpose you must tick the box "I accept the collection and processing of my personal data in order to benefit from the services" when creating your account.

Your consent is also required to share your personal data for commercial prospecting purposes. To this end, we ask you to tick the box "I agree to receive offers from MiQo's partners". You are free to withdraw your consent at any time or not to consent to the processing of your personal data when this processing is not necessary for the use of the services. We refer you systematically to this privacy policy which details the use, purposes and relevant information regarding the processing of your personal data.

WHAT TYPE OF DATA DO WE COLLECT?

In application of the Cameroonian, CEMAC zone and European regulations on data protection, we adopt the principle of minimization in the context of the collection of your personal data and only your data necessary for the purpose of the processing are collected.

DATA PROVIDED DURING YOUR REGISTRATION

Thus, in order to benefit from our services, we ask you to create an account (your "Account"). On this occasion, you must provide: your surname, first name, email address, telephone number, a profile photo, if applicable.

After creating your account in order to use our payment services allowing you to:





- Recharge your account;
- Receive payment;
- To transfer money ;
- Buy prepaid cards;
- Generate a virtual card
- Buy phone credit;
- Create and participate in savings pools;
- Pay bills online or at a local merchant;
- Buy communication credit;
- Access instant microloans;
- make savings;
- Access financial education articles and videos.

We ask you to provide us with additional information related to your payment card or your bank account IBAN.

DATA PROVIDED WHEN USING OUR SERVICES

In addition, in order to be able to carry out certain transactions or so that we can carry out certain checks on you, taking into account our obligation of vigilance with regard to the regulations relating to the fight against money laundering and the financing of terrorism, we may ask you to provide us with (i) proof of identity and (ii) proof of address.

Finally, we also collect the data of the beneficiaries of your transactions (surnames, first names, telephone number, payment card, IBAN, etc.), provided by you for the purposes of carrying out your payment transactions for their benefit (transfers, money transfers, payments).

DATA PROVIDED BY YOUR DEVICES

We collect data related to the device you use to connect to our services. (The model, operating system version, unique device identifiers and mobile network information, including your phone number). We may associate your device identifiers or phone number with your account.





We also record your usage data for our services from our website or mobile application. This usage data for our services from the website or mobile application. This usage data includes in particular all of your interactions with other users, all of the transactions that you carry out on our platform in a precise and dated manner.

When you use the functionality to locate MiQo agents geographically from the MiQo mobile application or the website, we collect information relating to your geographical location thanks in particular to your IP address or the GPS included in your devices.

COLLECTION OF COOKIES OR SIMILAR TECHNOLOGIES

By Cookies we mean the set of small alphanumeric files on your hard drive in order to recognize your device when you use our services. When you use our website or our mobile application, we can analyze your browsing, your movements and your viewing or consumption habits.

We place cookies on your device to simplify your navigation on our website or our mobile application or to personalize the advertisements that may appear during your navigation.

This operation allows us to offer you a more effective personalized visit and to make our communications or our advertising operations more relevant according to your centers of interest.

Like many websites, we automatically collect and store in log files information about your devices, including your IP address, the type of browser you use or your internet service provider.

Your consent is always required before any deposit of cookies and you can at any time oppose the use of these cookies by going to the "find out more" page containing the reference to opposition to tracking tools or by setting your browser.

However, this opposition to the use of cookies is likely to modify the conditions of access to our products and Services for the use of cookies.

However, the use of certain cookies does not require your consent.

These are cookies that are strictly necessary for the provision of services, such as: your transfer and authentication identifiers, certain audience analysis solutions (Analytics), etc.

We may also be required to use tags ("pixeltags") when sending electronic messages. This technology allows us to know if you have received and opened our messages and to reduce or remove sending from our messages.

A banner appears when you access our website or our mobile application, informing you of the use of cookies and the need to obtain your consent.





However, this banner disappears as soon as you continue browsing our website or our Mobile Application, i.e. until you go to another page or click on an element of the website or our mobile app.

Continuing to browse implies consent to the deposit of cookies on your device. The period of validity of your consent to the deposit of Cookies on your devices is 13 months.

HOW DO WE USE YOUR DATA ?

We aspire to create an attractive, efficient and personalized user experience, but always respecting the principles of loyalty and transparency. To this end, we use your data to:

IN ORDER TO PROVIDE PAYMENT SERVICES

Thus, we use your personal data in order to ensure the successful completion of the transactions that you choose to carry out for the benefit of beneficiaries or yourself, during the operation of (i) recharging your account (ii) collection of a payment (iii) money transfer (iv) purchase of prepaid cards (v) purchase of telephone credit (iv) creation and participation in pots (v) granting and access to nano-credits.

The data you provide allows us to carry out your payment transactions or to allow you to benefit from a payment transaction for your benefit by identifying you and identifying, where applicable, the beneficiaries of these transactions.

TO PROVIDE YOU WITH RECORDS OF YOUR TRANSACTIONS

We also collect and record the dates and times of your transactions in order to monitor their successful completion, prevent any complaints and provide you with a time-stamped statement of all your transactions.

IN ORDER TO GEOLOCATE YOU

When you choose to use the geolocation option of our agents, we use your information (IP address, GPS included in your devices) in order to (i) provide you with information on the location of these agents in relation to the where you are at the time of your request and (ii) to allow you to know in real time the number of agents present on a given perimeter and thus facilitate your payment transactions.



IN ORDER TO DEVELOP AND IMPROVE OUR SERVICES

We also use your personal data to help us create, develop, use or improve our products and services.

Thus, we can use your data to know the age of the user of the platform, your level of expenditure over a period, your rate of use of our services.

We may use your data that does not allow you to be identified to produce statistics, in particular on the amount of money transferred annually from the platform, the total number of users, or the rate of use of certain services.

We may also use your personal data for audit and research purposes in order to improve and personalize our offers or services and to provide you with a better experience.

TO COMMUNICATE WITH YOU

We also use your personal data to send you important notifications (by SMS, Mail) you cannot oppose, such as real-time notifications of your transactions made from your account, parent notifications of changes to our Terms and Conditions or this Privacy Policy.

We use your personal data to inform you of our news, offers from our partners when you have agreed to receive them.

We use your data to promote our services and increase its use or to respond to your requests through our customer service or to resolve your difficulties.

We may contact you by email, mobile phone, text, including push notifications, postings on our website or mobile app, or messages on your account.

TO PREVENT FRAUDULENT USE OF OUR ACCOUNT

We may, finally, use your personal data in the event of security necessity, in particular in the event of suspicion of fraud or attempted fraud. Thus, we collect and record your transaction data in order to detect and prevent any fraudulent use of your account and your payment data.

II. YOUR RIGHTS ON YOUR DATA

YOUR RIGHT TO INFORMATION

Indeed, the regulations of the CEMAC zone and Cameroon for data protection reinforce the obligation of information and transparency with regard to the persons whose personal data will be used, consequently, MiQo makes every effort to provide you with all the





information prescribed and detailed under the terms of this privacy policy. You have, in this respect, in particular the right of access, rectification, erasure, portability and limitation of the processing of your personal data. If in doubt, you can contact our customer service at any time at contact@mymiqo.com

YOUR RIGHT TO EXERCISE YOUR RIGHTS

HOW TO EXERCISE YOUR RIGHTS ON YOUR PERSONAL DATA ?

We make every effort to facilitate the exercise of your rights, access, rectification, erasure, portability and limitation of processing of your personal data.

We will always do our best to respond to each of your requests to exercise your rights and will make every effort to inform you of the measures taken following your requests within a maximum period of two (02) months from receipt of the request.

You can also, at any time via our internet or mobile platform in your personal space, send us your messages or make corrections or deletion to some of your personal data.

PERMISSION TO ACCESS

You can at any time access via your account your personal data including statements of your transactions and exporters in the form of a copy. We can also provide them to you in the event of a request to this effect made via your account or to contact@mymiqo.com accompanied by all relevant information allowing you to be identified (surname, first names, telephone number, email address).

RIGHT OF CORRECTION, DELETION

You can at any time rectify or delete your personal data included in your profile via your account on our internet or mobile platform or delete or modify specific elements, subject to the information that we keep within the legal or regulatory framework.

You can also send us any request to modify or delete your information at contact@mymiqo.com .

DATA PORTABILITY LAW

Created by the General Data Protection Regulation, the right to data portability is linked to the right of access to data. It gives data subjects the right to receive the personal data they have provided to a controller, in a structured, equally used and machine-readable format, in order to save them for further personal use and / or to transmit them to another controller without the first controller being able to prevent it.





Data may also be transferred directly from one controller to another at the request of the data subject, where technically feasible. If you wish to exercise your right to portability, you can send any request related to data portability to contact@mymiqa.com who will inform you in particular of the technical feasibility of this request.

III. SHARING YOUR PERSONAL DATA

DATA THAT YOU SHARE FROM YOUR ACCOUNT

Thanks to the platform's social network service, you can share information about yourself with other users of the platform, such as, in particular, your first and last names, telephone number, in order to communicate or interact with other users.

DATA WE SHARE WITH OUR BANKING PARTNERS

We share your personal data with our banking partners subject to professional secrecy, approved by the competent authorities as payment service providers and for which we are the duly mandated intermediary for the exercise of the profession of agent. payment service provider in the geographical area concerned.

This sharing made for purposes of control and provision of our services is essential use for its use.

You thus authorize, from the opening of your account and the subscription to our services, to exchange and share your personal data with our Banking partners.

When you choose to use the prepaid card purchase service, we share your data with our banking partner issuing the Prepaid Card. This sharing is essential to the provision of this service.

DATA WE SHARE WITH OUR SERVICE PROVIDERS

We may be required to call on third parties to provide certain services that we offer to you or to perform hosting, maintenance or marketing services for our services.

These third parties may have access to some of your personal information or data. Your personal data will always be governed by this Privacy Policy and your data will only be shared to provide you with our services or improve our products.

We also always make sure to put in place contracts that ensure the protection and confidentiality of your personal data as well as compliance with Cameroonian, CEMAC ZONE and European regulations on data protection.





We ensure in particular that contracts with third parties guarantee the non-use of your personal data for purposes other than those that we specify to them and the appropriate securing of your personal data in order in particular to prevent unauthorized processing, the loss or destruction of your personal data.

Thus, we ask our subcontractors for a commitment to use the data concerning you only for the purposes determined at the end of this Privacy Policy and only in accordance with our instructions.

We also require our subcontractors to implement security measures adapted to the sensitivity of the data that you communicate to us, in particular to prevent them from being distorted, damaged or communicated to unauthorized persons.

Finally, we prohibit our service providers, except with our prior written agreement, from subcontracting or transferring your personal data to a country that does not belong to the CEMAC zone. It is recalled that the notion of transfer also covers remote access.

DATA WE SHARE WITH OUR BUSINESS PARTNERS

Subject to your express acceptance, we may share your personal data with our business partners for marketing purposes.

This sharing never includes your payment information (Bank card, RIB, IBAN), or the supporting documents provided by you when opening your account and **cannot be carried out without your express agreement** materialized by ticking the box " **I accept to receive offers from MiQo's partners** ".

Subject to your express acceptance, our partners may thus be required to contact you in order to offer you specific offers. Under these conditions, in the event of your acceptance of their offers, our partners will act towards you as data controller with respect to the new contractual relationship created between you.

DATA WE DISCLOSE TO AUTHORITIES BY LAW

We may be required to share your personal data in particular when the law requires us to do so.

This may occur as part of our anti-money laundering and anti-terrorist financing due diligence obligation. We therefore have an obligation to monitor user payment transactions and alert the competent authorities in the event of an obvious anomaly in your transactions, whether at the stage of opening your account or in the context of its operation.

We may also be required to disclose your information in the context of an injunction or other legal action. This may be the case if we reasonably believe that this disclosure is





necessary in the context of an investigation into actual or suspected illegal activities, third party complaints, fraud or to ensure the security of our services. In such cases, we will endeavor to notify you except in an emergency or by order prohibiting us from doing so.

DATA WE SHARE IN CASE OF LOSS OF CONTROL OF THE COMPANY OR SALE

In the event of a merger, takeover or sale of ALCOFUND SA or a branch of activity, we may share your personal data with any third-party entity acquiring or integrating our company.

These operations can only be carried out in compliance with the regulations in force and this privacy policy.

IV. CONSERVATION OF YOUR DATA

HOW LONG DO WE KEEP YOUR DATA?

When we collect your personal data, we only retain it for as long as necessary for the purposes described under this privacy policy, unless a longer retention period is required by law.

DURATION OF CONSERVATION OF YOUR PAYMENT DATA?

As part of your payment transactions, we ask you to send us your payment card data.

The payment card number and the visual cryptogram are entered by you when carrying out your transactions.

However, we only make very limited use of this information. The retention period of your payment card data depends on the purposes pursued.

So, for a single payment, we keep your payment data only until the complete payment of your transactions.

Once the transaction is complete, we do not store or reuse your bank details with your express consent.

Nevertheless, all of your transactions are recorded and kept in our hard archives as proof, for a period of 13 months, corresponding to your time limit for contesting.

In addition, in order to facilitate your future transactions, we may ask you to authorize us to store data on your payment card.





This storage is necessarily subject to the collection of your prior and express consent. To do this, we ask you to tick the acceptance box provided for this purpose, when opening your account. On the other hand, the visual cryptogram appearing on the back of your card is never kept.

DURATION OF RETENTION OF YOUR IDENTITY AND DOMICILE DOCUMENTS

We may also, in the context of certain transactions and in order to comply with our obligation to monitor and analyze transactions in the context of the fight against money laundering and the financing of terrorism, you request proof of identity and address.

This information and documents are kept for a period of five years following the closure of your account.

DURATION OF CONSERVATION OF COOKIES AND IP ADDRESS

We keep cookies and other tracers placed on your hard drive in order to recognize your device when you use our services for a period of 13 months after which they are automatically deleted.

Regarding your IP address, it is deleted after 9 months.

ACCOUNTING STORAGE PERIOD

We may be required to keep your data for a longer period when the law requires it, in particular for accounting reasons relating to all the invoices that we issue or receive from you.

V. PROTECTION OF YOUR DATA

WHAT MEASURES DO WE IMPLEMENT TO PROTECT YOUR DATA?

The protection of your personal data is fundamental. Data security includes both their integrity, their confidentiality, and their availability.

As such, we implement security measures adapted to the sensitivity of the information you entrust to us, in particular to prevent it from being distorted, damaged or communicated to untrusted persons.





INFRASTRUCTURE SECURITY

In order to protect your data, we implement the technical and organizational measures carried out so that the processing meets the requirements of the GDPR, the CEMAC zone and Cameroon.

For the storage of your data we use the services of a host, using computer systems with limited access and whose premises use permanent physical security measures in order to protect and secure your data finally, your stored data is encrypted.

Our infrastructures incorporate regularly updated security software to protect your data against any introduction of malicious programs.

Thus, we protect and monitor your data in order to protect it from threats or malware, viruses and other forms of malicious code.

In particular, we make sure to always update the antivirus of our platform.

We implement all necessary security measures to protect your data against unauthorized access, modification, disclosure or destruction of the information we hold.

To this end, we conduct internal audits of data collection, storage and processing, including physical security measures, to prevent unauthorized access to our systems.

Access to your personal information is strictly limited to employees and contractors who need access to it in order to process it on our behalf.

Furthermore, any person having access to it is subject to strict confidentiality obligations and is likely to be subject to sanctions, in particular disciplinary sanctions, when it comes to an employee of the Company.

STRONG AUTHENTICATION

We protect your identifiers and passwords by requiring complex data (upper case, numbers, lower case) that we never store in clear, and invite you to renew them regularly.

In addition, we implement strong authentication to identify you, combining your password with your equipment (computer, mobile phone).

PAYMENT BY 3D SECURE

Regarding your payment transactions, these must necessarily be made by payment cards integrating the secure internet payment protocol, 3D Secure, which allows the bank issuing the payment card to authenticate the cardholder during payment. 'a payment and thereby limiting the risk of fraud.





PROCEDURE IMPLEMENTED IN CASE OF BREACH OF YOUR DATA

However, and despite all the security measures in place, we cannot guarantee the transfer of data via the public telecommunications networks used to access the services and in particular the Internet network, over which we have no control.

We can therefore only be bound by an obligation of means with regard to the confidentiality of the data during the transfer of these on the said public networks.

Consequently, unless proven negligence, on our part, we cannot in any case even be held liable in the event, in particular, of misappropriation, capture, corruption of your data or any other event likely to affect them, occurring during their transfer on public telecommunications networks, or fraudulent intrusion into its system.

Nevertheless, in the event of a violation observed relating to your data, we undertake to inform you as soon as possible when the violation is likely to create a high risk for your rights and freedoms.

This notification is accompanied by any useful information on the nature of the breach, the category of data concerned and their number, the probable consequences of the breach as well as the measures implemented to remedy it or mitigate any negative consequences.

VI. TRANSFER OF YOUR PERSONAL DATA

IS YOUR DATA TRANSFERRED OUTSIDE CAMEROON, THE CEMAC ZONE AND EU?

For the storage of your data we use the services of a localized host.

However, due to the organization of our Group, structured internationally, we inform you that the platform is likely to give limited access to some of your data to its employees, collaborators, or service providers located outside of Cameroon, CEMAC zone and EU.

In this context, we implement all measures to ensure that your data benefits from the same level of protection as that imposed by the Cameroonian, CEMAC ZONE and European regulations on data protection and we put in place clauses contractual guaranteeing a sufficient level of protection of your privacy and your fundamental rights.



VII. MANAGEMENT OF UPDATES AND REGULATIONS

HOW TO CONTACT US IN CASE OF COMPLAINT?

If you have any questions or concerns about this privacy policy or the way we process your personal data or if you wish to report any violation of your rights to us, you can contact us at contact@mymiqa.com .

Our team is at your disposal to answer you and resolve any difficulty you may encounter regarding the processing of your personal data. You can also submit any dispute or claim directly to the competent authorities, and if requested, we will endeavor to give you all the information on the remedies available to you.

HOW WILL YOU BE INFORMED OF UPDATES TO THIS PRIVACY POLICY?

We may modify or update this privacy policy. In the event of a substantial change, a notification will be posted on our internet platform or mobile application, accompanied by the updated privacy policy, supplemented by a notification. by email.