



PRIVACY POLICY

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

- Reload 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 prize pools;
- Pay bills online or at a local merchant;
- Buy communication credit;
- Access instant microloans;
- Make savings;
- Invest in assets with high added value;
- Access financial education articles and videos.

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

It is therefore incumbent upon us, and under our sole responsibility, to comply with the provisions of the regulations applicable in Canada and in particular as regards the collection of your prior consent to any processing of your personal data. We apply to any data processing carried out under our responsibility, the principles of lawfulness, loyalty, transparency, limitation of purposes, data minimization, accuracy, integrity, confidentiality and limitation in duration of retention of data concerning you.

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 data personal.





I. COLLECTION AND USE OF YOUR DATA PERSONAL

WHAT IS PERSONAL DATA?

The term "personal data" designates any information that can be used to identify you such as your name, postal address, email, or phone number for example.

YOUR CONSENT TO TREATMENT IS ALWAYS REQUIRED

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

Your consent is also required in order to share your personal data for the purposes of business development. To this end, we ask you to tick the box "I agree to receive offers from MiQo partners." You are free to revoke your consent at any time or to not to consent to the processing of your personal data when this processing is not necessary for use of services. We systematically refer you to this policy of confidentiality which details the use, purposes and relevant information concerning the processing of your personal data.

WHAT KIND OF DATA DO WE COLLECT?

In application of the European data protection regulation, 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"). TO this occasion you must provide: your name, first name, email address, phone number, a photo profile, if applicable.

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

- Reload your account;
- Receive payment;
- To transfer money;
- Buy prepaid cards;
- Generate a virtual card
- Buy phone credit;
- Create and participate in prize pools;
- Pay bills online or at a local merchant;
- Buy communication credit;





- Access instant microloans;
- Make savings;
- Invest in assets with high added value;
- 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 verifications with regard to you, taking into account our obligation of vigilance with regard to the regulations on the fight against money laundering and terrorist financing, we can help you ask 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, phone 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 THANKS TO YOUR DEVICES

We collect data about the device you use to connect to our services. (The model, operating system version, unique device identifiers and information relating to the mobile network, including your telephone number). We are likely to associate your device identifiers or your phone number on your account.

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

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

COLLECTION OF COOKIES OR SIMILAR TECHNOLOGIES

Cookies 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 consultation or consumption.

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

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

Like many websites, we automatically collect and store in files logs 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 cookies are placed and you can at any time oppose the use of these cookies by going to the "find out more" page containing the referral to tools for objecting to tracing or by configuring your browser.

However, this opposition to the use of cookies is likely to modify the conditions of access to our products and services use 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 identifiers assignment, authentication, certain audience analysis solutions (Analytics) etc.

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

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

However, this banner disappears as soon as you continue to browse our website or our Mobile Application, that is to say as long as you have not gone to another page or click on an element of the website or our mobile application.

The fact of continuing your navigation constitutes agreement to the deposit of cookies on your device. The duration 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 in the respect for the principles of loyalty and transparency. For this purpose, we use your data in order to:

TO PROVIDE PAYMENT SERVICES

Thus, we use your personal data to ensure the successful completion of the transactions you choose to realize for the benefit of beneficiaries or yourself, during the operation of (i) reloading your account (ii) receipt of payment (iii) money transfer (iv) purchase of prepaid cards (v) purchase of telephone credit (iv) creation and participation in saving pools (v) granting and access to nano-credits.

The data you provide us with are used to carry out your payment transactions or to send you benefit from a payment transaction for your benefit by identifying yourself and identifying, if applicable, the beneficiaries of these operations.

IN ORDER TO PROVIDE YOU WITH THE STATEMENTS OF YOUR TRANSACTIONS

We also collect and record the dates and times of your transactions in order to control their successful completion, to prevent any complaints and to provide you with a time-stamped statement of all of 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 (i) to provide you with information on the location of the these agents in relation to 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.

So, 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 which does not identify you to produce statistics, in particular on the amount of money transferred annually from the platform, the number total user, or the rate of use of certain services.

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

IN ORDER TO COMMUNICATE WITH YOU

We also use your personal data to send you important notifications (e.g., SMS, Mail) you cannot object, such as real-time notifications of your transactions from your account, parents' notifications of the modification of our general conditions or of this privacy policy.

We use your personal data to inform you about 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 resolve your difficulties.

We may contact you by email, phone on your mobile, SMS, including push notifications, by publications on our website or on the mobile application or by messages on your account.

TO PREVENT FRAUDULENT USE OF OUR ACCOUNT

Finally, we can use your personal data in the event of security necessity, in particular in the event of suspected fraud or attempted fraud. Thus, we collect and store your data transactions in order to detect and prevent any fraudulent use of your account and your data of payment.

II. YOUR RIGHTS OVER YOUR DATA

YOUR RIGHT TO INFORMATION

Indeed, the European regulation for data protection reinforces the obligation of information and transparency with regard to persons whose personal data will be played, accordingly, MiQo makes every effort to provide you with all the prescribed and detailed information under the terms of this privacy policy. In this regard, you have, in particular, the right of access, rectification, erasure, portability and limitation of the processing of your personal data. In case of doubt, you can contact our customer service at any time at contact@mymiqa.com

YOUR RIGHT TO EXERCISE YOUR RIGHTS

HOW TO EXERCISE YOUR RIGHTS OVER YOUR PERSONAL DATA?

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





We will always do our best to respond to each of your requests to exercise your rights and will do everything possible to keep you informed of the measures taken following your requests within a maximum of two (02) months from receipt of the request.

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

PERMISSION TO ACCESS

You can access your personal data at any time, including payment statements, through your account, your transactions and exporters in the form of a copy. We can also provide them to you in case of request to this effect formulate via your account or at contact@mymiqa.com accompanied by all relevant information allowing you to be identified (name, first names, telephone number, address E-mail).

RIGHT OF CORRECTION, DELETION

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

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

RIGHT OF DATA PORTABILITY

Created by Article 20 of 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 data of a personal nature that they have provided to a controller, in a structured format, also used and machine-readable, in order to save them for later personal use and / or to transmit them to another controller without the first controller can get in the way.

The data can also be directly from one controller to another at the request of the data subject, where technically possible. If you wish to exercise your right to portability you can address any request related to the portability of the data must be sent to contact@mymiqa.com who will inform you in particular about the technical feasibility of this request.

III. SHARING OF 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 names, telephone number, this in order to communicate or interact with other users.





DATA WE SHARE WITH OUR PARTNERS BANKING

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

This sharing, made for the purposes of monitoring and providing our services, is an 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 card partner issuing the Prepaid Card. This sharing is essential for the provision of this service.

DATA WE SHARE WITH OUR SERVICE PROVIDERS SERVICES

We may have to call on third parties to outsource certain services that we offer you or to perform hosting, maintenance or marketing services of our services.

These third parties may have access to some of your information or personal data. Your personal data will always be governed by this privacy policy and your data will not 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 European regulations on Data protection.

In particular, we ensure that contracts with third parties guarantee the non-use of your data. personal data for purposes other than those specified by us and the appropriate security of your data personal data, in particular to prevent unauthorized processing, loss or destruction of your personal data.

We therefore ask our subcontractors to make a commitment to only use your data. for the purposes determined at the end of this Privacy Policy and only according to our instructions.

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

Finally, we prohibit our service providers, unless we have prior written consent, from subcontracting or to transfer your personal data to a country that does not belong to the European Union. It is recalled that the notion of transfer also covers remote access.

DATA WE SHARE WITH OUR PARTNERS COMMERCIAL

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

This sharing never includes your payment information (Credit card, RIB, IBAN), or supporting documents provided by you when opening your account and **cannot be done without your express consent** materialized by checking the box " **I agree to receive offers from MiQo partners** ".





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

DATA THAT WE DISCLOSE TO AUTHORITIES BY LAW

We may have to share your personal data in particular when the law requires us to do so. This may occur as part of our duty of vigilance in the fight against money laundering and terrorist financing. We have, therefore, an obligation of surveillance user payment transactions and alerting the competent authorities in the event of an anomaly evident in your operations, whether at the stage of opening your account or in the context of its operation.

We may also be required to disclose your information as part of an injunction or any other judicial measure. This may be the case if we reasonably believe that such disclosure is necessary in the context of an investigation of proven 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 unless there is an emergency or an order prohibiting it.

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

In the event of a merger, control price or sale of ALCOFUND SA or a branch of activity, we may be required to share your personal data with any third-party entity acquiring or integrating our society.

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 keep it for as long as necessary for the purposes described in the terms of this privacy policy, unless a retention period longer is required by law.

DURATION OF RETENTION OF YOUR PAYMENT DATA?

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

The payment card number as well as the visual cryptogram are entered by you during the realization of your transactions.





However, we only make very limited use of this information. The shelf life of your payment card data depends on the purposes pursued. So, for a single payment, we only keep your payment data until payment has been made. complete your transactions.

Once the transaction has been completed, we do not keep or reuse your bank details thanks to your express consent.

However, a recording and conservation in our archives lasts raised of all your transactions is carried out as proof, for a period of 13 months, corresponding to your deadline, contestation.

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

This storage is obligatorily subject to the collection of your prior and express consent. For to do this, we ask you to check the acceptance box provided for this purpose, when opening your account. However, the visual cryptogram on the back of your card is never kept.

DURATION OF CONSERVATION OF YOUR PROOF OF IDENTITY AND DOMICILE

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

This information and documents are kept for a period of five years following the closing 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 RETENTION PERIOD

We may need to keep your data for a longer period when the law imposes it in particular for accounting reasons in relation to all the invoices that we issue or receive from you.

V. PROTECTION OF YOUR DATA

WHAT MEASURES ARE WE TAKING TO PROTECT YOUR DATA?

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

As such, we implement security measures adapted to the sensitivity of the information that you entrust us in order in particular to prevent them from being distorted, damaged or communicated to people not sure.





INFRASTRUCTURE SECURITY

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

For the storage of your data, we use the services of a host, using systems 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 integrated infrastructures security software regularly updated to protect your data against any introduction of Malware.

Thus, we protect and monitor your data in order to protect them 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 any unauthorized access, modification, disclosure or destruction of the information we hold.

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

Access to your personal information is strictly reserved for employees and subcontractors who have need to access them in order to process them on our behalf.

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

STRONG AUTHENTICATION

We protect your usernames and passwords by requiring complex data (capital letters, numbers, lowercase) that we never store in clear, and invite you to renew them regularly.

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

PAYMENT BY 3D SECURE

Regarding your payment transactions, they must necessarily be made by credit cards, payment integrating the secure internet payment protocol, 3D Secure, which allows the bank to card issuer to authenticate the card holder during a payment and limit thus the risks of fraud.

PROCEDURE IMPLEMENTED IN THE EVENT OF A BREACH OF YOUR DATA

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

We can therefore only be bound by an obligation of means regarding the confidentiality of data when they are transferred over said public networks.





Consequently, except proven negligence, on our part, we will not be able in any case even our liability incurred in the event, in particular, of misappropriation, capture or corruption of your data or any other event likely to affect these, occurring during their transfer to the public telecommunications networks, or fraudulent intrusion into its system.

However, in the event of a violation noted 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 violation, the category of data concerned and their number, the probable consequences of the breach as well as the measures taken implemented to remedy or mitigate any negative consequences.

VI. TRANSFER OF YOUR PERSONAL DATA

IS YOUR DATA TRANSFERRED OUTSIDE THE EU?

For the storage of your data, we use the services of a local host. However, due to the organization of our Group, structured internationally, we inform that the platform is likely to give limited access to some of your data to its employees, collaborators, or service providers located outside Canada and Cameroon.

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

VII. MANAGEMENT OF UPDATES AND REGULATIONS

HOW TO CONTACT US IN CASE OF A CLAIM?

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

Our team is at your disposal to answer you and resolve any difficulty you may have required to meet regarding the processing of your personal data. You can also transmit any dispute or claim directly to the competent authorities, and in the event of request we will do our best to provide you with all information on the remedies available to you.

HOW WILL YOU BE INFORMED OF THE UPDATE OF THIS PRIVACY POLICY?

We may need to modify or update this privacy policy, In the event of substantial modification, a notification will be displayed on our internet platform or mobile application, accompanied by the updated privacy policy, completed by email notification.

