



PRIVACY POLICY

PRIVACY POLICY VER. 1.0

Document Information

Document Property	Document Details
Document Title:	Privacy Policy
Document file name:	Privacy Policy VER. 1.0
Revision Number:	Version 1.0
Issued by:	Monesto Bank
Issue date:	25/02/2026
Status:	Final

Document Revision History

Version	Date	Author	Description of change
1.0			First issued version

1. Contents

1.	CONTENTS	3
2.	BASIC PROVISIONS	4
3.	DATA CONTROLLER. DATA PROTECTION OFFICER. AUTHORITY AND WEBSITE.....	5
4.	 GROUNDS FOR PERSONAL DATA PROCESSING	5
5.	PERSONAL DATA STORAGE	6
6.	PERSONAL DATA TRANSFER	6
7.	PERSONAL DATA PROCESSED	8
8.	YOUR RIGHTS SUBJECT TO YOUR PERSONAL DATA PROCESSING	10
9.	PERSONAL DATA RECIPIENTS	11
10.	WEBSITE AND COOKIES	12

2. Basic Provisions

We, **Monesto Bank**, duly incorporated and operating under the laws of the Union of the Comoros (hereinafter also referred to as the **Company** or **We**).

Full details are: Monesto Bank, License number L16229/MB

Company number 16229, Date of incorporation: 30.12.2025

Registered address: Boulevard de Coalancanthe, Mutsamudu, Anjouan, Union of Comoros

We have developed this Privacy Policy (hereinafter also referred to as **the Policy**) which sets out the basis on which any personal data collected from our Customers, or that our Customers provide to us by using our Services, will be processed by us.

Monesto Bank is committed to protecting the confidentiality, integrity, and lawful use of personal data entrusted to it by clients, partners, employees, and other data subjects.

For the purposes of this Policy, **personal data** means any information relating to an identified or identifiable natural person - **data subject**. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

We irrevocably presume, that by submitting your personal data to us, you agree to such data transfer, storing and processing. We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Policy.

We assume that before using our website or becoming our Customer you have read this Policy and have accepted its terms and provisions.

This is the most recent version of the Policy. We reserve the right to make amendments and/or update this Policy from time to time, including new data processing and safety practices and guidelines. The Policy is to be updated as and when necessary, and must be reviewed at least once a year, considering legislative changes, as well as changes in Company's strategy, operation or external circumstances affecting the its Services.

We are committed to protecting and respecting our Customers privacy, complying with applicable data protection laws and regulations and thus ensuring the protection and confidentiality of personal data.

We ensure that your personal data are being processed based on:

- The Constitution of the Union of the Comoros (2018), Article 24 – safeguarding the right to privacy
- Law No. 14-029/AU on the Protection of Personal Data (2021)
- Law No. 13-003/AU on Banking Regulation – professional secrecy
- Law No. 21-012/AU on Cybersecurity and Cybercrime – protection against unauthorized access to personal data
- AML/CFT Law No. 12-008/AU (as amended by Law No. 21-004/AU) – lawful disclosure for anti-money laundering purposes
- Decree No. 23-074/PR on Targeted Financial Sanctions – data processing related to sanctions obligations
- Applicable directives and circulars issued by the Central Bank of the Comoros (BCC)
- European Union Rules for the protection of personal data, including data protection inside and outside EU, as the best practices.

3. Data Controller. Data Protection Officer. Authority And Website

Monesto Bank acts as the primary data controller responsible for the handling and protection of personal data it processes in the course of its business activities.

Legal address: Boulevard de Coalancanthe, Mutsamudu, Anjouan, Union of Comoros

Email (data protection matters): compliance.control@monesto.io

Data Protection Officer (DPO): compliance.control@monesto.io

You can at any time obtain information about your personal data available to us, about how we collect, use and store your personal data or exercise your other rights as the data subject. In this regard please contact us by emailing to the above email.

Our **Data Protection Officer** is a well-trained and highly experienced, is involved in all matters related to personal data processing. In addition, the Data Protection Officer is responsible for ensuring communication with Customers, as well as with the supervisory authorities regarding personal data processing.

Please do not hesitate to contact our Data Protection Officer with any questions regarding your personal data and this Privacy Policy

4. Grounds For Personal Data Processing

The Company is entitled to process your personal data only in the following events:

- we have previously determined the purposes of processing of your personal data
- we have determined the amount of your personal data required to accomplish the pre-determined purpose
- we have defined legal basis to process your personal data and
- we have provided you with information on your rights within the context of personal data processing.

Usually we process your personal data according to the standard procedure based on:

- necessity to render Services to our Customers and enter into respective agreement (establishment of business relationships, inter alia, when you remotely register with us to use Services provided by the Company)
- necessity to fulfil legal obligations applicable to us, inter alia, but not limited to, Anti Money Laundering and Counter Terrorism Financing legally binding obligations subject to Customers due diligence and Know Your Customer purposes (inter alia, for the purposes of Customers' identification and verification, due diligence and know your customer procedures under obligations stipulated in the respective legal regulations applicable to the Company). These personal data processing purposes mainly are stipulated by the Money Laundering and Terrorist Financing Prevention acts of the United Kingdom
- consideration of legitimate interests of the Company or a third party
- risk assessment and management
- your consent to process your personal data (inter alia, when you sign up for any news or other information using our website).

Legal Framework

This Policy is based on the following legal instruments:

- **Constitution (2018), Art. 24:** guarantees the right to privacy and confidentiality of communications
- **Law No. 14-029/AU (2021):** regulates personal data protection, including obligations of data controllers and rights of data subjects
- **Law No. 13-003/AU (2013):** imposes banking secrecy and confidentiality obligations on all bank staff
- **Law No. 12-008/AU (2012), as amended by Law No. 21-004/AU (2021):** requires financial institutions to disclose data in the context of AML/CFT investigations
- **Law No. 21-012/AU (2021):** defines and penalizes cyber offenses and mandates cybersecurity standards
- **Decree No. 23-074/PR (2023):** implements targeted financial sanctions, obligating asset freezes and data disclosure
- **Bank of Comoros Circulars and Guidance:** particularly related to AML/CFT compliance and risk management

5. Personal Data Storage

We perform your personal data processing during the validity term of business relationships between us and after termination of business relationships, in order to fulfil requirements under applicable law and regulations and in order of protection of our legitimate interests.

We are entitled to store your personal data **for 5 (five) years** as from the moment of termination of business relationships unless the laws and regulations set other time- limits for storing the personal data.

We shall ensure centralised storage of personal data and data masking/erasure after expiry of the mandatory storage period according to the applicable legislative and regulatory acts. If there are obstacles for these actions (e.g., order on the prohibition of data erasure), data storage shall be ensured until the elimination or cancellation of these obstacles.

When assessing the personal data storage duration, we take into account the requirements of the applicable legislative and regulatory acts, contractual obligation fulfilment aspects, your instructions (for instance, in the case of consent) as well as our legitimate interests. If your personal data is no longer required for the purposes specified, we will erase or destroy it. We shall have the right to determine a new purpose for certain personal data in certain cases, if arising due to regulatory enactments or, or if is required in order to protect of our legal interests.

6. Personal Data Transfer

Please note that the Company in no events rents or sells your personal data to anyone.

We will transmit your personal data to third parties only in cases directly allowed by the applicable laws and regulations, only with the aim to provide our Services and exclusively on the base of special agreement entered between and by the Company and respective third party, which includes nondisclosure and secure exchange provisions.

The third parties in question belong to the following categories: banking and payment operators, internet providers, companies specialising in IT and SMS services; companies that carry out KYC/AML database checks and fraud database checks.

We may also be required to share your personal data with various financial institutions and/or enforcement or court authorities to comply with Anti-Money Laundering, Terrorist Financing and Transfer of Funds laws and regulations, prevent fraud, enforce an agreement we have with you, or to protect our rights, property or safety, or the rights, property or safety of our employees or others.

Additionally, we may reveal your personal data to third-parties if:

- you request or authorize it
- to address emergencies or acts of God and
- to address disputes, claims, or to persons demonstrating legal authority to act on your behalf.
- Transfer of your personal data to third countries (outside the Comoros, European Union (EU) and European Economic Area (EEA) and international organisations is possible based on:
 - the laws of Comoros;
 - decision made by the European Commission regarding the level of protection of a third country's personal data, available here: https://ec.europa.eu/info/law/law-topic/data-protection_en
 - relevant guarantees (for example, applying binding corporate rules or standard personal data protection clauses adopted by the European Community)\
- exceptional legal grounds.

The Company will only send your personal data outside the UK, EU/EEA to a country having the adequacy of its security level and which does not provide the corresponding guarantees, if:

- You have clearly agreed to the proposed transfer, having received information from us about the potential risks that such a transfer could pose to you;
- Transfer is necessary in order to fulfil the agreement between the us and
- Customer or to implement measures after the conclusion of the agreement, which were approved at Customer's request;
- Transfer is necessary for conclusion of an agreement between us and another
- private individual or legal entity, in the interests of the person or for the fulfilment of such an agreement;
- Transfer is necessary if there are important reasons of public interest;
- Transfer is necessary in order to raise, fulfil or defend legal requirements, or
- Transfer is necessary in order to protect the vitally important interests of Customer if Customer is physically or legally incapable of giving its consent.

We may also obtain information from other sources and combine that with information we collect through our Services. For example, we may collect information about you from **third parties**, including but not limited to social media platforms and publicly available sources: public court documents, the ROC and the company houses and registers of other jurisdictions, and from electronic data searches, online KYC search tools (which may be subscription or license based), anti-fraud databases and other third party databases, sanctions list, outsourced third-party KYC providers and from general searches carried out via online search engines (e.g. Google).

In all events we carefully select personal data processors and, when making data transfer, we

evaluate its necessity and the amount of data to be transferred. Data transfer to processors is carried out subject to the requirements of confidentiality and secure processing of personal data.

7. Personal Data Processed

To provide you with Services that meet your needs, we use various personal data, including audio and video recordings, IP addresses and etc., subject to the legal obligations arising mainly from the **Money Laundering and Terrorist Financing Prevention acts of the United Kingdom and European Union regulations**.

The personal data processed by the Company are grouped into categories to manage them in the most efficient way and for you to be able to see the amount of Customer information managed by us.

Personal data categories	Description
Basic (identification/verification) data	Name, surname, former name (-s), identity number, date of birth, picture, copy of your Identity document, proof of residence, language of communication, e-mail address, phone number, audio/video records, selfie, etc.
Profiling and data characterising the behaviour and habits	For the purposes of Customers' Anti Money Laundering risk assessment and management, the Company performs Customers profiling to detect the respective risk profile of the Customer. In this regard we are mandatory obliged to consider various factors subject to Customer and its transaction - age, gender, nationality, citizenship/residence, information on personal/business activity, geographic location, education, employment, professional skills, aim of business relationships establishment, the origin of funds, source of wealth, etc. We do not involve automated decision-making in personal data processing for Customer's profiling purposes.
Financial data	Information on income and assets, proposed turnover and amount of transactions, nature of transactions, tax information, etc.
Special Category Data	Information on a politically exposed person, sanction list, criminal records, bankruptcy, insolvency, bailiff claims, and etc.

Data obtained when fulfilling legal obligations	Information obtained upon request of investigating authorities, tax authorities, bailiffs, etc.
Transaction data	Business partners and parties to the transactions, including, but not limited, bank details: account number, SWIFT, BIC, card information (card number, CVC or CVV, card expire date, card holder Name and Surname), transactions amounts sent and received, amounts paid for the Services, respective contracts and invoices. Transaction Data includes also details about: (i) the type of virtual financial assets involved, the order volume, price, value; (ii) your virtual currency exchanging records; (iii) transaction history on the platform, including withdrawals and virtual and fiat currency exchanging; (iv) amounts credited to your account and your account balances. Transaction Data also includes ongoing monitoring results of transactions performed or intended to be performed.
Tele- and e-communication data	Phone number, e-mail, social media (LinkedIn, Twitter, Facebook), Skype, Website and etc.
Authentication details	Technical/LOG data - user name, password, login, device type, browser type, time zone settings and location, session time, PIN code, IP address (VPN), details of electronic stamp, etc. Contact Us Data – data received when Customers communicate with us by means of our website, including email address, name, other data subject to question applied.

We may request, obtain, collect personal data from Customer itself or its representatives, authorised persons, or other persons related to Customer (if any), or from public and private registers or other third persons.

We shall ensure confidentiality of personal data, protect it from unauthorised access, illegal processing disclosure, accidental change (amendments, corrections), loss or destruction by implementing organisational and technical measures in accordance with the requirements of the applicable law and regulations.

8. Your Rights Subject to Your Personal Data Processing

The Company hereby irrevocable accepts that the following rights are granted by the effective legislation to the Customer subject to personal data processing:

- to access your personal data and forward them – in particular, you are entitled:
 - to obtain additional information about the processing of your personal data irrespective of what type of information you already have
 - to receive an electronic copy of your personal data processed by us.
- to amend or delete your personal data – it means that:
 - you are entitled to amend your personal data if they have changed or you have grounds to believe that your personal data processed by us are not accurate.
- to request the Company to delete your personal data, and we will do it if we are not prohibited to do so subject to provisions of applicable legal acts and regulations and we do not need these personal data anymore for the purposes which the data were collected or processed in any other way.
 - to limit the processing of your personal data:
- you are entitled to request the Company to limit the processing of your personal data (or certain processing activities), which means that we could
 - store and process your personal data only to establish, exercise or defend our legal claims
 - you are entitled to limit the processing of your personal data in cases when:
 - they are not accurate
 - they are being processed unlawfully but you do not want to delete them,
 - their processing is not required anymore but you want to establish, exercise or defend your legal claims
 - you have already exercised your right to object to the processing of your personal data but you are waiting for our assessment whether we are entitled to further process your
 - personal data based on our or third party's legitimate interests.
- to object to the processing of your personal data:
 - you are entitled to object to the processing of your personal data if the objection is based on serving the Company or third party's legitimate interests, and your rights, interests and freedoms are more important than our said or third party's legitimate interests.
- to be informed about a new purpose of data processing in advance:
 - you are entitled to receive information on whether the provision of personal data is related to the law or an agreement, whether the provision of data is a precondition for the conclusion of an agreement, as well as information that the subject is required to provide personal data, and consequences in case such data are not provided
- in relation to the automated individual decisions, including profiling:
 - you are entitled to make our specialist participate in taking such decisions or request that we do not take a decision based on an automated calculation only.
 - to lodge a complaint with the appropriate data protecting authority if you have concerns about how We process your personal data.
 - to revoke your given consent on your personal data processing.

Regarding your access to personal data, please note, that reasonable access to your personal data will be provided at no cost upon request made at e-mail address:

compliance.control@monesto.io

If access cannot be provided within a reasonable time frame, we will provide you with a date when the information will be provided. If for some reason access is denied, we will provide an explanation as to why access has been denied.

9. Personal Data Recipients

We are entitled to disclose your personal data to the following recipients:

- members of management bodies, employees, representatives, authorised persons of the Company
- public institutions, public officials, investigatory authorities, courts, prosecutor's office, subjects of operational activities, orphans' courts, notaries, law enforcement officials, judicial and investigatory authorities of other member states and foreign countries, tax authorities, arbitration courts, out-of-court dispute resolution bodies — financial market participants (correspondent banks, insurance companies, payment systems, credit registers, securities registers, agency companies, stock exchanges, depositories, business partners of the Company or Customers, financial service intermediaries etc.)
- the Company's cooperation partners, agents, suppliers and service providers, auditors, advisors.

10. Website And Cookies

Our website is monesto.io

The purpose of our Website is to keep its visitors informed about Company's business, provided Services and terms and conditions of usage thereof.

Our Website may include links to **third party** websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you.

We do not control these third-party websites and are not responsible for their privacy notices, statements or policies. We encourage you to read the Privacy Policy of every website you visit.

Our website is not intended for minors and we do not collect personal data relating to minors. In case we recognize that we have collected personal data from a child, we shall delete that information as quickly as possible. If you suppose that a child under 13 may have provided us a personal data, please contact us.

We use cookies on our website. Cookies are small files that a site or its service provider transfers to your computer's hard drive through your Web browser (if you allow) that enables the site's or service provider's systems to recognize your browser and capture and remember certain information.

We use the following cookies:

- **session cookie** – are necessary for ensuring the security and technical functionality. Cookies are not stored and are processed only during the actual website visiting time

- **persistent cookie** – remembers information about the visitor's actions, such as language settings, login information or the statistics information about routing of the
- website visitors.
- **third party cookie** – analytical software such as **Google Analytics** cookies, which by analysing the data allows to track the visitors between two or more websites and offers
- more appropriate website connections.

Any information gathered by cookies is stored only until cookie expiration dates and is not used for any purposes other than those specifically mentioned

Each time you visit our website from a new IP address, you have the right to accept or reject the processing of cookies.