

DATA PROTECTION POLICY

(Version 1.1 – 6 Aug 2024)

1. INTRODUCTION

We are committed to handling personal data in a fair, secure, and transparent manner. We are also committed to enabling you to efficiently exercise your rights over your personal data.

This Policy (“**Policy**”) explains how we, Monty Finance SAL (“**we**”, “**us**” or “**our**”), collect, use, disclose, and process your personal data when you use our website www.mymonty.com.lb (“**Website**”), our mobile application MyMonty (“**App**”), and any of the services available to you through our Website or App (collectively, the “**Services**”). It also explains your rights as data subject and their protection.

By continuing your interactions with us, such as by using our Services or providing information to us, you confirm that you understand and agree to the collection, use, disclosure, and processing of your personal data (or the personal data of any other individual you provide) as described in this Policy.

2. WHAT IS PERSONAL DATA, PROCESSING, AND SENSITIVE PERSONAL DATA?

“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.

“Processing” means any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means. Thus, processing includes: collecting, recording, organizing, structuring, storing, adapting, altering, retrieving, viewing, using, disclosing, transmitting, disseminating, making available, aligning, combining, mirroring, replicating, restricting, erasing or destroying.

“Sensitive personal data” refers to any personal data that may reveal information about a person’s racial or ethnic origin, political opinion, religious beliefs, trade union activities, physical or mental health, sexual life and orientation, genetic or biometric data, data relating to criminal convictions and offences.

3. OUR DATA PROTECTION PRINCIPLES

We collect and process personal data lawfully, fairly and in a transparent way.

We collect your personal data only for valid purposes that were clearly communicated to you and do not process it in any way that is incompatible with those purposes.

We avoid the collection and processing of sensitive personal data, unless required otherwise.

Personal data we collect will be relevant to the purposes announced and limited only to those purposes.

Personal data we collect will be accurate and kept up to date.

We keep personal data only as long as necessary for the purposes announced or as required by applicable legal/regulatory requirements.

We securely process personal data with the appropriate technical and organizational measures.

4. WHAT ARE YOUR RIGHTS AS A DATA SUBJECT?

In the age of data, regulators all over the world are aiming to grant data subjects sufficient ownership and control over their personal data. Thus, you have protected rights in regards to the collection and processing of your personal data, subject to applicable laws and regulations. These rights include:

- The right to access personal data.
- The right to request the correction or the updating of personal data without undue delay.
- The right to request the erasure or the destruction of personal data^(*) ^(**).
- The right to object to or to restrict the processing of personal data^(*).
- The right to data portability. You may request a readable copy (including, where applicable, by machine) of all the personal data you provided to us.
- The right to withdraw consent at any time regarding the processing of personal data. For example, you may require us not to use your personal data for marketing purposes^(*).
- The right to be informed on how the data that has been collected, on how it is going to be used, for how long it will be kept and whether it is going to be shared with any third parties.

^(*) By exercising this right, we may not be able to offer you products and services or to pursue our relationship with you.

^(**) Subject to legal and regulatory requirements which might prevent us from granting such a request.

Your data shall be accurate and up to date. Please help us by informing us promptly of any changes to your personal circumstances or details.

You can exercise your rights at any time by submitting a written request. All requests relating to such rights will be dealt with promptly in accordance with applicable laws and regulations.

5. HOW IS DATA COLLECTED AND PROCESSED?

The categories of personal data that we collect and process depend on the extent and circumstances of the relationship with you and the products or services requested and/or performed.

Data collection through different channels

We collect and process different categories of personal data, which we receive from you in person or via our communication channels, including our online channels.

Our website uses small text files stored in a user's browser files known as cookies. Cookies are used to improve our website functionalities and also to improve the experience of our users. In order to find out information about how we use cookies please refer to our [Cookies Policy](#).

We may also collect and process personal data which we lawfully obtain from other third parties (e.g. credit reference agencies, risk and compliance intelligence databases, filtering systems, public authorities).

We may also collect and process personal data from publicly available sources (e.g. official governmental portals, trade registers, press, media and online databases) which we lawfully obtain and are permitted to process.

Types of collected and processed data

When you wish to become our customer and wish to obtain some of our products and services and when you use such products and services, personal data collected and processed may include:

- Identification and contact data: first name, last name, middle name, parents' names, place and date of birth, ID number, ID documents (ID card, passport, etc.), residence address, professional address, mailing address, email, telephone number, e-signature.
- Family status: marital status, number of children, spouse name and occupation.
- Employment information: occupation, name of employer, professional income.
- Electronic information, specifically: identity, authentication, technical logs, connection security, IP address, etc.
- Financial and transactional data: assets, revenues, IBAN, card number, transaction data, loans and credits, engagements, etc.
- Data in relation with habits and preferences in connection with our products and services.
- Data related to the interactions with us: video surveillance, recorded calls, email exchange, chats via support channels.

For prospective customers, or non-customer counterparties in a transaction with our customer, a guarantor, a security provider, a legal representative of a customer or an authorized representative of a legal entity, we may collect relevant personal data which may include, inter alia, the following:

- Name, address, contact details, identification data, date and place of birth, nationality, marital status, employment status, authentication data you need to access our digital platforms.

- For guarantors, we will request personal data disclosing their economic and financial background and their credit status with other financial institutions.

6. WHAT IS THE LEGAL BASIS FOR COLLECTING AND PROCESSING PERSONAL DATA?

Understanding that personal information and the right to privacy are extremely valuable to individuals and are protected by law, we do not collect or process personal information without making sure we have a proper legal basis to doing so.

For the performance of a contract

We collect and process personal data for the purposes of concluding and performing contracts for financial transactions with our customers and to offer them suitable financial services and products as well as other ancillary services. We also collect and process such data to be able to complete our acceptance procedure of prospective customers.

For compliance with a legal obligation

Several legal and regulatory obligations prescribed by relevant Lebanese and international applicable laws and regulations (commercial and financial regulations, anti-money laundering rules, tax rules, etc.) require us to collect and process personal data. This processing fulfills our obligations in terms of:

- Complying with legal obligations and regulatory requirements.
- Fighting money laundering, terrorism financing and financial crime.
- Complying with international sanctions.
- Fighting tax evasion.
- Risk management (credit risk, cyber risk, etc.).

For the purposes of our legitimate interests

We collect and process personal data for the purposes of fulfilling our legitimate interests. For example:

- We collect and process personal data as part of establishing legal files to be used in litigation if legal proceedings take place.
- We collect and process personal data as part of our physical and IT security systems for the prevention of potential crime, unauthorized access and for physical and asset security, admittance controls and anti-trespassing measures including the setting up of Video Surveillance systems (CCTV) for the prevention of crime or fraud.

7. HOW DOES THE PERSONAL DATA FLOWS AND WHO DO WE SHARE IT WITH?

In offering our products and services, we may provide personal data to various divisions and departments within our company.

Personal data may also be shared with service providers and suppliers enabling us to perform our services. These service providers and suppliers are bound by contractual agreements with us compelling them to comply with banking secrecy, confidentiality and data protection requirements.

The following recipients are examples of service providers and suppliers to whom personal data may be transferred:

- Merchants whose merchandise/services is being purchased via the electronic wallet (e.g. Monty Mobile for e-Sim purchases via the electronic wallet).
- Aggregators of electronic vouchers available for purchase via the electronic wallet.
- Third parties to whom the electronic wallet user is settling due bills (e.g. Touch, Alfa and Ogero)
- Remittance service providers, in the context of the execution of local and cross-border transactions.
- Cards processing companies in the context of offering data subjects card services.
- Debt collection agencies and credit reference agencies.
- External legal consultants and attorneys and external auditors.
- File storage, archiving and/or records management companies.
- IT companies in the context of implementing, operating, maintaining, and upgrading IT systems including core systems, AML systems, ID verification systems etc.
- Websites and advertising agencies.
- Partner insurance companies in the context of gathering required data in in the context of processing certain claims related to our staff.

We are also bound to transfer personal data to supervisory authorities and other regulatory and public authorities as per the applicable laws and regulations. For example, personal data may be transferred to:

- Banque du Liban in the context of processing certain transactions.
- The Banking Control Commission (BCCL) and the Special Investigation Commission (SIC) in the context of their respective supervisory role and control missions, and when answering specific requests.

Personal data may also be transferred to processors in third countries. Such processors are under the obligation to comply with the data protection principles, and we will only disclose personal information to third parties providing an adequate level of protection.

8. WHAT CAN YOU DO TO HELP US KEEP YOUR DATA SAFE?

We do our utmost efforts to protect your personal data, but there are certain things that you can do too, such as:

- Install anti-virus software, anti-spyware software and a firewall, and keep them updated.
- Do not leave your device unattended.

- Immediately report any security incident/breach related to our services and products (such as the loss of your card or compromise of your account or email address to our call center or customer support to take immediate protective action(s).
- Log off from the online application when you are not using it.
- Keep your passwords strictly confidential and use strong passwords.
- Be alert online and learn how to spot unusual activity, such as a new website address or phishing emails or chats requesting you to provide your personal information.

9. HOW DO WE STORE YOUR PERSONAL DATA AND FOR HOW LONG?

We store collected personal data mainly in electronic format. We may store personal data in paper format from time to time.

The stored data in both formats is securely retained by us in accordance with the applicable laws and regulations and with our security policies and procedures.

The retention period complies with local and international applicable laws and regulations' requirements.

The retention period may be extended as required by a competent authority or if needed in the context of defending a right or a legitimate interest.

Most of the collected personal data is retained for the period covering the contractual relation and, in any case, for a period of 10 years as of the date of the relation's end.

We will only retain personal data for as long as necessary to fulfill the purposes it was collected for, including those of satisfying any legal, accounting, or reporting requirements.

10. HOW DO WE PROTECT YOUR PERSONAL DATA?

We take all appropriate and lawful technical, physical, legal and organizational measures against accidental or unlawful processing of data including destruction, loss, alteration, dissemination or access.

We have a strict access right policy in place governing our employees' access to our premises and IT systems. The IT Security team actively enforces the applicable security policy and monitors any breaches thereof.

In this context, we remind you to always keep your credentials private (wallet number, card number, card PIN, username, password, etc.) and recommend that you always make sure to keep your physical cards within your sight while performing a transaction with a merchant, and to sign out of the application at the end of each session. We also make sure, whenever possible, to implement two factor authentication mechanisms.

If we believe that your personal data may have been compromised, we notify you as soon as possible in accordance with applicable laws and regulations.

If you have reason to believe that your personal data has been compromised, you should notify us immediately.

11. SAFEGUARDS IN PLACE TO PROTECT YOUR PERSONAL DATA

We may anonymize or aggregate personal information in such a way as to ensure individuals cannot be identified from it.

We may use anonymized/aggregated data for statistical analysis and administration including analysis of trends, to tailor our business and our service offerings, to conduct risk assessment and to analyze costs and charges.

We may share anonymized/aggregated data with the third parties mentioned in this document.

12. WHO TO CONTACT IN RELATION WITH PERSONAL DATA PROTECTION?

If you have questions or queries about this data protection policy, and wish to exercise your rights or to file a complaint, or to report an incident you can contact our Data Protection Officer (DPO) to this end, using this e-mail address: dpo@montyfinance.com

Requests will be handled swiftly and with confidentiality.

13. COMPLAINTS

If you are unhappy about our management or the handling of your personal data you are entitled to file a complaint at complaints@montyfinance.com.

14. CHANGES TO THIS POLICY

To ensure we're always in tune with the latest laws, following the best practices, and changes in how we handle your personal information, we may revise this Policy from time to time. Any updates will be shared by posting a revised version on our Website.