

USER AGREEMENT

1. INTRODUCTION

This User Agreement (“Agreement”) governs your access to the platform to store, exchange virtual currencies to virtual currencies and trade on a peer to peer matching service enabling you to buy and sell virtual currencies from other customers. The services on the platform are provided by the operating company Wallet Services (hereinafter: “Wallet”, “us”; “we”) to you (hereinafter: the “User”, “Customer”, “you”).

Before using Wallet, you agree that you have read, understood, and accepted all of the terms and conditions contained in this Agreement and in our Privacy Policy and Anti-Money Laundering/Combating the Financing of Terrorism Policy (AML/CFT Policy).

Please read this Agreement carefully before using Wallet. Your access to and use of Wallet is subject to your compliance with this Agreement.

The terms of this Agreement apply to all users and others who access or use Wallet. If you do not agree to accept and abide by any of the terms of this Agreement, or if the Agreement conflicts with your national law or the law of your location, you agree not to use Wallet. If you fail to do so, you will be liable for all losses and damages to Wallet or third parties caused by your failure to comply with the Agreement.

In addition, when using particular Wallet services, you are subject to any published guidelines or rules applicable to such services, as may be published and amended from time to time.

Wallet does not provide any fiat related services nor holds any fiat money for or on behalf of its Customers. Wallet displays Customer’s virtual currency balance and transaction amounts in fiat currency type preliminarily chosen by the Customer in the settings of Wallet, for Customer convenience purposes only.

Transactions in virtual currencies are high-risk transactions. Before investing in any virtual currencies, you should analyze all the possible risks associated with virtual currencies. All virtual currencies available in Wallet are operated by third parties, Wallet is not affiliated, has no direct or indirect control over or any ability to influence such third parties. Thus, keep in mind that some virtual currencies may depreciate completely and become unavailable in Wallet. Wallet is not responsible for sharp fluctuations in virtual currency, its drop in value, depreciation, removal from Wallet, and other risks associated with virtual currency transactions.

2. CHANGES

We may from time to time, at our discretion, make changes and improvements to this Agreement. By continuing to use Wallet after these changes have been made, you express and acknowledge your consent to the changes.

3. SERVICES PROVIDED

Wallet is a platform that allows you to exchange virtual currencies to virtual currencies, deposit, withdraw, store virtual currencies and trade on a peer to peer matching service (hereinafter: the “Service”, “Services”) Please be aware that certain functionality available on Wallet, namely: exchanging fiat currency into virtual

currency and exchanging virtual currency into fiat currency is provided through third parties with whom Wallet has partnered (“Third party services”). Your use of Third party services, apart from this Agreement will also generally be subject to separate terms and conditions set forth by relevant third party service providers. It is your responsibility to understand the terms and conditions of Third Party services, including how those service providers use any of your information under their privacy policies. Wallet is not responsible for Third party service providers actions or inactions.

4. HOW TO USE WALLET

In order to be entitled to access and use the Services, you represent and warrant that:

- The Services provided by Wallet are offered in response to your own initiative and request. By accessing and using our platform, you acknowledge and agree that you have independently sought out our services without any active solicitation or marketing efforts on our part. This transaction is initiated at your own discretion, and you understand that Wallet has not actively solicited or promoted its services to you. Your use of our platform constitutes your confirmation that this transaction is based on your independent decision and initiative.
- You are at least 18 years old and have reached the legal age in accordance with the applicable jurisdiction.
- You are an individual of full legal capacity and physical capacity and have sufficient authority to agree to this Agreement.
- You are the lawful owner of the funds used to receive the Services in connection with this Agreement, and these funds come from legal sources.
- You do not provide us with misrepresenting, misleading, false, or fraudulent information.
- You have not previously been banned or restricted from using our Service.
- You are not in breach of any of the provisions of this Agreement or applicable laws and regulations.
- You are not a person on the United States Treasury Department’s List of Specially Designated Nationals or the U.S. Department of Commerce Denied Persons List, and you are not subject to European Union or United Kingdom Treasury sanctions or another foreign sanctions regime.
- You are not located in, or a resident or national of, the United States, an unrecognized country or territory, or a jurisdiction requiring a mandatory national license or registration for virtual currency operators, or special registration, which Wallet may not have.
- You are not located in, or you are a resident or national of, a country blacklisted by the Financial Action Task Force (FATF).
- You are not using Tor (The Onion Router), VPNs (virtual private networks) to misrepresent your IP address and/or location.

It is your responsibility to ensure that you comply with the relevant laws in your territory of residence (registration) and/or the territory of your residence from which you are accessing Wallet.

USDT functionality is not available to users based in mainland US, US territories, or US citizens and Prohibited Countries as defined under Tether's Terms of Service.

In addition, Wallet reserves the right to restrict or prohibit the use of Wallet for certain jurisdictions if required by applicable law or our AML/CFT Policy provides for such restriction or prohibition in which case Wallet is not liable for any losses or damages incurred by you due to your inability to access Wallet.

5. WALLET REGISTRATION PROCEDURE

i. Making a request.

To start using Wallet, you must activate Wallet and provide Wallet with personal details from your Telegram profile.

ii. User verification and transaction monitoring.

Wallet takes the necessary steps to comply with applicable Anti-Money Laundering and counter terrorist financing legislation, as detailed in the AML/CFT Policy, which is an integral part of this Agreement.

We reserve the right to restrict or block your access to Wallet, freeze your virtual currencies, and postpone any transaction if we detect a risk of fraud or illegal activity. We may also require you to provide additional information or wait for a period of time after the transaction has been completed before allowing you to use any Wallet Services and/or before allowing you to make transactions outside certain limits. For more information, see the "Suspension, Termination, and Cancellation" section of this Agreement.

When accessing Third party services you give your consent to the sharing of your personal information between Wallet and its partners and understand that Wallet has the right to restrict your access to the Service and Third party services based on information received from its partners.

6. PROHIBITED USE

We grant you a limited, non-exclusive, non-transferable license, subject to the terms and conditions of this Agreement, to access and use the Service and related content, materials, and information (collectively" the "Content") solely for the purposes permitted by this Agreement.

Any other use of the Service or the Content is expressly prohibited, and all other rights, titles, and other rights in the Service or Content belong exclusively to Wallet and its licensors.

You agree that you will not copy, transmit, distribute, sell, license, reverse engineer, modify, publish, or participate in the transmission or sale or otherwise use any Content for the purposes other than permitted by this Agreement, in whole or in part.

Wallet draws your attention to the fact that transactions related to illicit activities, obfuscating funds, illegal services, fraudulent schemes, pyramids, dark net, extortion, money laundering, terrorist financing, subjects of sanctions regimes, and other categories of unacceptable risk for Wallet are prohibited. Wallet performs blockchain analysis of transactions and reserves the right to freeze funds if suspicious transactions are detected and to report to the competent authorities as required by local AML/CFT legislation.

7. SUSPENSION, TERMINATION AND CANCELLATION

Wallet may suspend, restrict or terminate your access to any or all of the Services and/or Third party services if a valid subpoena, court order, or compulsory order from a public authority so requires.

And/or we reasonably suspect you of prohibited use of Wallet.

And/or the use of your Wallet account is subject to any legal proceedings, investigation, or government proceedings.

And/or we believe that there is an increased risk of non-compliance with legal or regulatory requirements relating to your use of Wallet.

And/or our service partners cannot support your use of the Third party services.

And/or you take actions that, in our sole discretion, circumvent the rules and controls we have established, including, but not limited to, opening multiple Wallet accounts, or abusing promotions that Wallet may offer from time to time, *or* you are in breach of this Agreement and other Wallet policies.

You can also notify Wallet of your wish to stop accessing Wallet at any time by sending a request to the support team @wallet_supportbot.

8. RESOLUTION OF COMPLAINTS

If you have any feedback, questions, or complaints, please contact us @wallet_supportbot.

If you have a complaint, please state the reason for your complaint, how you would like us to resolve the complaint, and any other information you consider relevant. We will investigate your complaint based on the information you have provided and any information provided by Wallet.

Your complaint will be dealt with within a reasonable time.

The agent may make the following decisions based on your complaint:

- To resolve your complaint as you have asked.
- To decide whether or not to reject your complaint and state the reasons for the rejection.
- To offer to resolve your complaint with an alternative solution.

You agree to use the complaints procedure described in this section before bringing any action to a competent court. Failure to comply with this provision may be used as evidence of your unwillingness to settle the matter out of court and/or the inadmissible nature of the complaint.

9. USER VERIFICATION AND LIMITS

In certain cases required by local AML/CFT legislation, Wallet is required to identify and verify its Customers and monitor their activities and transactions. In certain cases, including when you exceed internally set transaction limits, Wallet will also be required to request additional information from you, including answers to questions about how you expressed interest in the virtual currency, the purpose of the transactions, the source of wealth or funds, including documentary evidence.

In addition to the situation of exceeding internal limits, Wallet may, at its discretion, conduct additional verification of the User in the event of suspected activity as set out under the “Suspension, Termination, and Cancellation” section of this Agreement.

Wallet may change the applicable limits and restrictions at any time and at its own discretion. Wallet may, at its sole discretion, modify the applicable restrictions if it believes that the Customer's actions violate applicable laws, the company's AML/CFT policy, or this Agreement.

You acknowledge that Wallet's decision to restrict your transactions or access the Service may be based on the confidential criteria which are essential for Wallet's risk management and security protocols. You also acknowledge that Wallet has no obligation to disclose the details of the risk management and security procedures to you unless otherwise provided in the Privacy Policy.

10. WARRANTIES AND RESPONSIBILITIES OF THE PARTIES

Data transmission to Wallet is encrypted using SSH, HTTPS, and SSL/TLS. No method of transfer or electronic storage is 100% secure; therefore, we cannot guarantee its absolute security.

By using Wallet, you agree that Wallet is not responsible for any consequences arising from the use of information provided by Wallet.

Wallet will not sell, buy, provide, exchange, or otherwise disclose your data, transaction details, or personal information about the User or to anyone other than the partners and third parties set out in the Privacy Policy.

Secure access to your custodial virtual wallet in Wallet must be ensured by yourself. Wallet accepts no responsibility for unauthorized access or unauthorized management of virtual currencies in your virtual currency wallet provided by Wallet Services. You must take all precautions to limit unauthorized access to your account and you are responsible for taking appropriate security measures to access your Telegram account. If you lose access to your Telegram account or if your Telegram ID in Telegram is deleted, you may permanently lose access to the virtual currencies stored in your custodial wallet in Wallet.

We are not responsible for any circumstances that affect the transaction after the virtual currency has been sent to the address you have provided. If there is confirmation on the blockchain that the virtual currency has been sent, our obligations will be treated as fully discharged.

You are responsible for the correctness of the virtual wallet address you provide in the event of loss of virtual currency if the address proves to be incorrect, invalid, or unsuitable for a particular type of virtual currency.

It is also your own responsibility to update your contact details to receive any notifications or warnings we may send you. We will not be liable for your failure to observe or comply with any notices or warnings that we may send you.

We accept no responsibility for any damage or interruption caused by any computer viruses, spyware, scareware, Trojans, worms, or other malicious software that may affect your computer or other equipment, or any phishing, spoofing, or other attacks. We recommend the regular use of verified and easily accessible virus-checking and prevention software.

Although Wallet takes all necessary and reasonable measures to keep the Services up and running, Users use it at their own risk.

The Services are provided without any representations or warranties of any kind, express or implied, as required by law with respect to the software or websites, including but not limited to warranties or conditions of quality, performance, non-infringement, merchantability, and fitness for a particular purpose.

We do not represent or warrant that we or any other associated software will always be available, uninterrupted, timely, secure, accurate, complete, and error-free or will operate without loss.

Subject to this section, Wallet will not be liable for any loss or damage arising out of or in connection with the use of the Services, even if the Services has been advised and/or made aware of the possibility of such loss or damage. In particular, the Service is not responsible for:

- Loss of any actual or anticipated profit, income, or any indirect, special, incidental, or consequential damages and loss of opportunity.
- Any indirect, special, incidental, or consequential damages.
- Any damage to the data (direct or indirect).
- Loss of goodwill (direct or indirect).
- We will not be liable for delays, failures, or interruptions in service, which result directly or indirectly from any cause or condition beyond our reasonable control, including but not limited to any delay or failure caused by any act of God, an act of civil or military authority, an act of terrorism, civil unrest, war, strike or other labor dispute, fire, interruption of telecommunications or internet services or network provider services, equipment and/or software failure, cyberattack or another disaster or any other event that is beyond our reasonable control and does not affect the validity and applicability of any of the other provisions.

11. FINAL CLAUSES

Wallet does not provide general or personal financial advice to Users. Nothing in Wallet is intended or should be taken as financial, legal, or tax advice. Users should seek personal financial, legal, tax, and accounting advice from third-party professionals about the likely outcomes for them in using the Service.

The meanings of terms, conditions, and representations contained herein will be subject to definitions and interpretations in English. Any translation provided may not accurately reflect the information in the original English.

ANTI-MONEY LAUNDERING/COMBATING THE FINANCING OF TERRORISM POLICY

(AML/CFT Policy)

1. Introduction

Wallet has robust policies in place aimed at preventing financial crimes, money laundering and the financing of terrorist activities. Wallet is committed to demonstrate its engagement to prevent financial crimes, comply with regulations, protect financial systems, maintain a good reputation, mitigate risks, and foster international cooperation.

2. Principles of customer due diligence

Wallet applies due diligence measures to customers, business relationships, and transactions and monitors business relationships on an ongoing basis.

Due diligence measures include:

a) Identifying the customer's identity on the basis of documents, data, or information obtained from a reliable and independent source or from any other source that Wallet has reasonable grounds to rely on and can be relied upon to identify and verify the customer's identity.

b) Obtaining information on the purpose and intended nature of the business relationship and establishing details of the customer or beneficial owner to enable Wallet to identify:

- Complicated or unusually large transactions;

- Unusual transaction patterns that have no apparent economic or visible legitimate purpose; or

- Any other activity that, by its nature, may be related to money laundering, terrorist financing, or other criminal conduct.

2.1. Terms of due diligence measures

Wallet conducts due diligence before or during the course of establishing a business relationship with customers or conducting a one-off transaction.

Wallet may, after conducting risk-management procedures, complete due diligence on a customer after establishing a business relationship if:

a) It is necessary in order not to interrupt the normal conduct of business.

b) There is no reasonably certain and reasonable suspicion of money laundering or terrorist financing.

It is understood that due diligence measures will be completed by Wallet as soon as possible.

Wallet may apply simplified due diligence measures to specific business relationships or transactions if Wallet determines that the business relationship or transaction presents a low risk of money laundering and terrorist financing.

Where money laundering and terrorist financing are suspected, Wallet does not apply such measures.

2.2. Application of due diligence measures

Wallet takes a holistic view on Customer's profile and activity. We conduct Customer risk assessment and take into consideration different criteria, related notably to the customer profile, geography and location, transactions and channels of communication to decide when and which degree of due diligence measures shall be applied.

Due diligence measures apply when:

- a) It establishes a business relationship with the customer;
- b) It doubts the accuracy or adequacy of documents, data, or information obtained for the purpose of identifying or verifying the customer; or
- c) There is a reasonable suspicion of money laundering, terrorist financing, or other criminal behavior.

Notwithstanding the above, Wallet's due diligence measures apply to existing customers at appropriate times based on customer risk and at our own discretion.

2.3. Application of enhanced due diligence measures

The result of Customer risk assessment may lead to the application of enhanced due diligence measures. Wallet applies risk-based enhanced customer due diligence and enhanced ongoing monitoring in addition to due diligence measures in situations that, by their nature, present a higher risk of money laundering, terrorist financing, or other criminal conduct, or in relation to business relationships with persons from countries that do not or do not fully apply the Financial Action Task Force recommendations.

Such measures include:

- a) Establishing the source of wealth and the source of funds related to the proposed business relationship or one-off transaction;
- b) Seeking additional independent, reliable sources to verify the information provided by Wallet;
- c) Taking additional steps to understand the background, ownership, and financial situation of the customer and other parties to the transaction.
- d) Taking further steps to ensure that the transaction is fit for purpose and in line with the intended nature of the business relationship;
- e) Strengthening control over business relationships, including closer monitoring of transactions.

3. CONTINUOUS MONITORING

Wallet constantly monitors its customers and their transactions.

Ongoing monitoring of business relationships means:

- a) Scrutinizing transactions carried out throughout the business relationship to ensure that these transactions are consistent with Wallet's knowledge of the customer and the risks and source of the customer's funds.
- b) Keeping up-to-date documents, data, or information obtained in order to apply customer due diligence measures.

4. TERMINATION OBLIGATIONS

Where, in respect of any Customer, Wallet is unable to apply due diligence measures in accordance with this Policy, Wallet will:

- a) Not carry out the transaction with or on behalf of the customer.
- b) Not establish a business relationship and not carry out one-off transactions with the customer.
- c) Terminate any existing business relationship with the customer.

If Wallet cannot continuously monitor a business relationship, Wallet will terminate that business relationship. In some cases, Wallet may be required to file reports with the relevant authorities.

Wallet applies applicable international sanctions and pays special attention to all its customers, their activities, and facts that indicate the possibility that a customer is the subject of international sanctions.

5. RESTRICTED JURISDICTIONS

The United States of America (USA), Democratic People's Republic of Korea, Iran, Afghanistan, Haiti, Liberia, Libya, Mali, Myanmar, Somalia, South Sudan, Syrian Arab Republic, Yemen, Cuba.

Wallet reserves the right to choose markets and jurisdictions in which it operates, and may also restrict or refuse provision of its services in other countries, territories or regions if deemed to have risk at our own discretion or required by laws, competent authorities or sanctions programs.

You should inform us immediately if you become a resident in any of the above restricted jurisdictions. You understand and acknowledge that if it is determined that you have given false representations of your location or place of residence, Wallet reserves the right to take any appropriate actions with compliance to the local jurisdiction, including termination of your access to Wallet.

6. CHANGES TO THIS POLICY

Wallet has the right to amend this AML/CFT Policy. If the current version is amended, the date of the last update of the new Policy will take effect from the date of its publication, unless otherwise provided for in the new AML/CFT Policy.

PRIVACY POLICY

1. GENERAL PROVISIONS

1.1. The organization responsible for data processing is Wallet.

1.2. Personal data collected by Wallet is processed in accordance with local legal requirements, the General Data Protection Regulation (“GDPR”), and other legal regulations.

1.3. Wallet, in accordance with applicable legal requirements, ensures the confidentiality of personal data and implements appropriate technical and organizational measures to protect personal data from unauthorized access, disclosure, accidental loss, alteration, destruction, or other unlawful processing.

1.4. This Privacy Policy sets out our current policies and obligations regarding data protection and privacy. Accordingly, we endeavor to collect and process only data that is strictly necessary in the context of our interaction with (potential) customers, (future) partners, users/visitors of our Services and online resources, to provide services and/or information for specific and legitimate purposes.

1.5. We are posting our Privacy Policy on Wallet in its most current version. Please read it carefully.

By accessing and using Wallet, you acknowledge that you have read, understood, and agree to this Privacy Policy.

1.6. This Privacy Policy is an integral part of the user agreement posted on Wallet and is mandatory for use of the Services hosted on Wallet.

1.7. Wallet reserves the right, in its sole discretion, to change this Privacy Policy at any time by posting an updated version of the Privacy Policy on Wallet and, if the changes are material, notifying users. A modified or updated version of this Privacy Policy will take effect as soon as it is posted on Wallet.

2. TYPES OF DATA WE COLLECT

2.1. The primary purpose for which Wallet collects your personal data is to grant you access to use Wallet (“Services”). We need to collect and store your personal data in order to provide our Services to you, comply with laws, and improve our Services.

2.2. Wallet will collect and process the following data:

2.2.1. The information you provide to us.

You may provide us with information about yourself when you register to use our Services, such as when you provide us with personal details, such as your Telegram username, profile name, URL-photo, Telegram ID and phone number. This also includes information you provide by continuing to use our Services, participating in a promotion or survey, and reporting problems with our Services.

The information you give us may include your name, date of birth, address, telephone number, identification information (such as proof of identity and nationality), and financial information.

2.2.2. The information about you that we collect.

Regarding your use of our Services, Wallet may automatically collect the following information:

- Details of the transactions you make when using our Services
- Technical information, your registration details, operating system, and platform.

2.2.3. Information we collect from other sources.

Wallet may receive information that you pass on to third parties when using the Wallet Service — e.g., from an online payment service or user verification organization. Third parties other than Wallet may process users' personal data set out in Section 6 of this Policy.

2.3. Data retention period: Unless otherwise required by law, you agree that we have the right, but not the obligation, to retain all personal data collected for the duration of your use of our Services and for the period required by law, but no longer than 7 years.

2.4. We do not collect information from anyone under the age of 18. If you are under 18 years old, you may not provide us with any personal information or use Wallet Services.

3. HOW WE PROTECT YOUR PERSONAL DATA

3.1. Wallet keeps your personal data secure by using secure storage with industry-standard encryption. We have also implemented a number of security measures to ensure that your information is not lost, misused, or altered, including but not limited to the following:

3.1.1. Physical Measures

Tangible media containing your personal data will be kept in a locked room.

3.1.2. Electronic Measures

Computer data containing your personal data will be stored on computer systems and on tangible data carriers that are secured by strict log-in restrictions.

3.1.3. Management Measures

Only authorized employees are permitted to come into contact with your personal data, and such employees have undertaken to comply with our internal privacy policy.

3.1.4. Technical Measures

Encryption technology can be used to transmit and store your personal data. We use the various security technologies and controls currently available to minimize the risk that your personal data may be disclosed, corrupted, misused, obtained without authorization, disclosed without authorization, or altered. Our technical security team actively monitors abnormal and malicious activity on our servers and Services.

3.1.5. Other Measures

We are committed to protecting your information from unauthorized access, alteration, disclosure, or destruction of the personal data we collect and store.

We take various measures to ensure information security, including:

- Encrypting our communications with you.
- A periodic review of our methods for collecting, storing, and processing personal data.
- Limited access to your personal data based on necessary knowledge for our employees and suppliers, who are subject to strict contractual confidentiality obligations.

3.2. Please note that it is not possible to guarantee 100% security of your data. You are therefore asked to take measures to protect your personal data yourself.

3.3. You agree that Wallet will not be liable for any loss of information or other damage not caused by our intent or gross negligence, including but not limited to hacking, power outage, or unavoidable technical failure, to the maximum extent permitted by law.

3.4. If you suspect that your personal data has been compromised, please contact us immediately.

4. METHODS OF USING YOUR PERSONAL DATA

4.1. We use the information we collect about you for the following purposes or in the following ways:

4.1.1. To provide our Services

Wallet uses the data collected to fulfill its obligations regarding you, provide you with information, products and services, and verify your identity.

4.1.2. For your and our protection

We use the information we collect to protect our platforms, user accounts, and archives, and protect against automated abuses, such as spam, phishing, and DDoS attacks.

We analyze your activity on our Services to identify suspicious behavior as early as possible to prevent potential fraud and loss of funds by bad participants.

4.1.3. To comply with legal requirements

Regarding privacy and security of personal data, Wallet will use the information in accordance with its legal obligations, government requests, and reasonable user requests.

4.1.4. For research and development

Wallet actively measures and analyzes data to administer its Services and for internal operations, including troubleshooting, data analysis, testing, research, statistical and survey purposes, and understand how you use and interact with our Services.

This review is conducted by our operations teams to continually improve our Services and troubleshoot user interface issues. Also, Wallet uses such information to customize, measure, and improve our Services, the content and layout of our websites, and to develop new services.

We constantly monitor activity in our systems and our communications with users to look for and quickly rectify problems.

4.1.5. To communicate with you

Without collecting and processing your personal data to confirm each message, Wallet will not be able to respond to requests you send.

All messages are properly retained by Wallet or by a service provider appointed by Wallet to check for accuracy, to be held as evidence or used to meet other legal or contractual obligations.

4.1.6. To ensure compliance with our User Agreement

The information collected is also used for ongoing and proactive enforcement of our terms and conditions, including but not limited to reviewing, investigating, and preventing any potentially prohibited or illegal activity that may violate the above provisions, or disclosing relevant information to a third party in accordance therewith.

Wallet reserves the right to suspend or terminate any Services to any user found to be in breach of our terms and conditions.

4.1.7. For marketing and advertising

Wallet may share your personal data with our marketing partners for targeting, modeling, and/or analytics, marketing and advertising purposes.

4.1.8. For other purposes

Wallet may disclose your personal data for any other purpose for which you have given additional consent by signing a written document or completing an electronic form provided by the operator.

5. LEGAL BASIS FOR PROCESSING

5.1. When we process your personal data, we will rely on one of the legal bases for processing below. We may process your personal data on several legitimate grounds, depending on the specific purpose for which we use your data.

5.1.1. Execution of the contract

When necessary, Wallet may process personal data if the processing of your personal data is necessary to fulfill its obligations under the User Agreement we have entered into with you.

5.1.2. Legal obligation or in the public interest

Wallet is required to process your personal data in accordance with legal obligations.

The purposes of the processing include identity verification controls, money laundering and fraud prevention, risk control measures, and providing information to a competent authority, public authority or law enforcement agency.

5.1.3. Legitimate interests

Where necessary, Wallet may process personal data where we, or a third party, have a legitimate interest in pursuing commercial and business interests, unless such interests override your interests, fundamental rights, and freedoms.

5.1.4. Your consent

In certain circumstances, Wallet may ask you for specific permission to process personal information for certain purposes.

Your data will be processed in this way if you agree to this. If the legal basis is the consent you have given, you can withdraw your consent at any time. Withdrawing your consent will not affect the legitimacy of the data processed before the withdrawal.

6. WHO RECEIVES YOUR PERSONAL DATA

6.1. Wallet receives your personal data in order to fulfill your requests and services and to comply with our contractual and legal obligations.

6.2. We share your personal data with third parties if this is necessary for our legitimate business needs, to fulfill requests, and to provide services and/or as required or permitted by law. Third parties in such circumstances include:

6.2.1. Service providers

Wallet will disclose personal data to third-party partners and service providers (processors) so that they can process it on our behalf where appropriate. These service providers are obliged to provide sufficient safeguards under data protection law — e.g., by being bound by contractual obligations regarding confidentiality and data protection. We will only pass on the personal information they need to provide their services.

6.2.2. Auditors and consultants

We may disclose personal data for the purposes and in the context of audits — e.g., external audits, security audits — to legal and other consultants to investigate security concerns, risks, complaints, etc.

6.2.3. Supervisory bodies, law enforcement agencies, courts

Wallet may disclose personal data in accordance with applicable law and regulatory obligations to respond to requests from regulatory authorities, government and law enforcement agencies, courts, and court orders.

6.2.4. Other persons

Other recipients can be any individuals or legal entities to whom you ask for your data to be transferred — e.g., a link, etc., give your consent to the transfer of personal data or it's necessary to provide you with Services.

6.3. Wallet may also disclose your data in the following circumstances:

- If we are under a duty to disclose or share your personal data in accordance with any legal or regulatory obligation or request.
- To enforce or apply the terms and conditions or any other agreement in force in the context of our relationship and to investigate potential breaches.
- In order to protect our rights, safety, or property, or the rights of our customers or third parties/public. This includes sharing information with other companies and organizations for the purposes of money laundering, fraud prevention, and similar risks.

7. TRANSFERS OUTSIDE THE EEA OR TO INTERNATIONAL ORGANIZATIONS

The above applies to the personal data of European Union users.

7.1. Your personal data may be transferred to third countries (outside the EEA) or international organizations if the transfer is necessary and has a legal basis as described in this document. Such transfers take place, for example:

- When it needs to be done in the context of the Services.
- In accordance with applicable law.
- Based on your instructions or consent.
- In the context of data processing carried out by third parties on our behalf (for example, data may also be processed by staff working outside the EEA who work for Wallet or for one of our third-party service providers. These employees may have technical and support duties, duties related to processing your orders, providing support services, etc.).

7.2. Processors (or controllers) in third countries, in this case, must either be approved by the European Commission as providing an adequate level of data protection or must have appropriate safeguards corresponding to the EU level of data protection. We are committed to taking all steps reasonably necessary to ensure that your data is treated securely.

8. YOUR RIGHTS

8.1. Under applicable law, you have the right to access the information we hold about you. Your right to access can be exercised in accordance with relevant data protection legislation. If you have any questions about our use of your personal information, please contact us. Under certain conditions, you may require us to:

- Provide you with more information about how we use your personal data.
- Provide you with a copy of the data you have given us.
- Update any inaccurate, incorrect, or outdated personal data we hold.
- Delete any personal data that is no longer necessary or no longer subject to the legal obligations to which Wallet is subject.
- If the processing is based on your consent, withdraw your consent so that we stop that particular processing.

- Stop direct marketing with you by contacting us.
- Where we carry out fully automated decision-making that results in a legal obligation or similarly significant impact, you can request information from us on the decision-making methodology and ask us to verify that the automated decision has been correctly made. We may refuse a request as permitted by applicable law, including where providing the information would disclose a trade secret or prevent or detect fraud or other crime. However, as a general rule, in these circumstances, we will check that the algorithm and source data are functioning as expected, without error or distortion, or, if required by law, to correct the processing.
- Object to any processing on the basis of legitimate interests, unless our reasons for such processing outweigh any prejudice to your data protection rights.
- Limit the use of your information during the investigation of a complaint.

8.2. When you exercise these rights, there are certain exceptions to protect the public interest — e.g., preventing or detecting crime — and our interests — e.g., maintaining legal privilege.

9. RIGHT TO LODGE A COMPLAINT

9.1. If you have any complaints about the use of your data, please let us know and/or make a complaint using the contact details below. We will investigate immediately and inform you of the outcome.

9.2. Complaints should be written in English in a comprehensive manner and contain sufficient detail and a clear description of the complaint. Wallet will not be able to handle requests that are incomprehensible or in languages other than English.

9.3. You can also lodge a complaint with the competent territorial supervisory authorities, but if the complaint has not been sent to us in advance, we can use this fact as evidence of your unwillingness to settle the matter out of court.

10. CHANGES TO OUR PRIVACY POLICY

To keep up with changing legislation, best practices, and changes in the processing of personal data, we may update this Privacy Policy from time to time as appropriate to the circumstances.

If we make material changes to this Privacy Policy, we will notify you by email and provide you with an updated Privacy Policy. If required by applicable law, we will obtain your explicit consent for material changes.

11. CONTACTS

11.1. Please send any questions, comments, or requests regarding this Privacy Policy to the support team at Wallet.

13.2. If you believe that we have not adequately addressed your questions or concerns, or you believe that your data protection or privacy rights may have been violated, you may file a complaint with any supervisory authority or other government agency responsible for enforcing privacy laws.