Wafee Privacy Policy

This Privacy Policy describes the policies and procedures of Wafee ("We", "Our", "Services", "Company", or "Us") pertaining to the collection, use, and disclosure of user's information through mobile applications, products and services we offer ("Wafee app").

We are committed to protect the privacy of our users, as privacy is considered to be the fundamental right of the users.

We respect your privacy, value its importance, and are wholly committed to keeping your information safe and secure. We process your personal data in accordance with privacy laws and this Privacy Policy to make sure your data protection rights are implemented and enforceable.

We understand that your personal data is important to you, so we have implemented different technical and organizational solutions to comply with applicable legislation related to the processing of your personal data, privacy and security in countries where we operate or where the applicable law applies to us.

Further, we are committed to protecting the privacy of our clients, customers, and website visitors. As such, we have implemented policies and procedures to ensure that we comply with the GDPR and other applicable data protection laws and regulations.

The Privacy Policy sets forth the basic rules and principles by which we process your personal data, and mentions our responsibilities while processing your personal data according to transparency obligations

This Privacy Policy applies to all personal information that we collect, use, and process in the course of our business activities, including information collected through our website. It explains how we process personal data, what we do with it, and how we keep it secure.

We understand that your personal data is important to you, and we take our responsibility to protect it seriously. We are committed to being transparent about our data processing practices, and we strive to provide clear and concise information to help you understand how we use your personal data.

We recognize that data protection is an ongoing process, and we are committed to continuously improving our practices to ensure that we meet the highest standards of data protection and privacy. If you have any questions or concerns about our privacy practices, please do not hesitate to contact us.

Read this Privacy Policy carefully and understand how your personal data is treated by us. By accessing any of our services and the services offered by our third parties you consent and agree to the collection, transfer, storage, disclosure, and the use of your data as described in this Privacy Policy. IF YOU DO NOT AGREE WITH THIS POLICY, PLEASE DO NOT USE OUR SERVICES.

1. Introduction

At Wafee, we provide a seamless banking experience that integrates Fiat and Crypto functionalities effortlessly. With our innovative app, users can create IBAN accounts in multiple currencies, perfectly complementing their Wafee card and crypto addresses. Whether you need to send, receive, or top up your payment cards, Wafee ensures a smooth and hassle-free experience.

For businesses, we offer specialized Business IBAN accounts, equipped with features such as mass payments, crypto issuance, and fiat currency conversion – all designed to streamline your business banking operations.

With integrated IBAN functionality, Wafee empowers you to manage multi-currency accounts, conduct crypto and fiat transactions, and enjoy low-cost international transfers – all from the convenience of your smartphone. With Wafee, you're in complete control of your financial assets.

Experience banking like never before with Wafee – your passport to a smoother, faster, and more convenient banking journey.

2. Scope of the Privacy Policy

This privacy policy applies to all personal data processed by us in connection with the Services, including personal data collected through our website, mobile applications, and other digital or offline means. It also applies to personal data collected from our clients, partners, vendors, and other third parties.

3. Definitions

As used herein, the following terms are defined by GDPR as follows:

"**Consent**" means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

"**Controller**" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

"**Data Portability**" means the right of a data subject to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.

"**Data Protection Officer (DPO)**" means a person designated by the controller or processor to oversee data protection strategy and implementation, and to act as a point of contact for data subjects and supervisory authorities.

"**Data Subject**" means the individual to whom the personal data relates.

"**Personal data**" means any information relating to an identified or identifiable natural person (data subject).

"**Processing**" means any operation or set of operations performed on personal data, such as collection, recording, organization, structuring, storage, adaptation, or disclosure by transmission, dissemination or otherwise making available, erasure, or destruction.

"**Processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

"**Supervisory authority**" means an independent public authority responsible for monitoring the application of the GDPR, including investigating complaints and conducting audits and inspections.

4. Information we collect

For the purpose of this Privacy Policy, Personal Data means information that relates to an identified or identifiable natural person.

We collect various types of Personal Data when you use our services.

Personal data can include a wide range of information, such as an individual's name, address, email address, phone number, date of birth, social security number, health information, and biometric data. It can also include information about an individual's preferences, behavior, and interactions with others.
An identified natural person is someone who can be identified, directly or indirectly, by reference to an identifier such as a name, identification number, location data, online identifier, or other factors that are specific to that person.

Under the General Data Protection Regulation (GDPR), personal data is protected as a fundamental right. Controllers and processors shall ensure that personal data is processed lawfully, fairly, and transparently, and that it is collected for specified, explicit, and legitimate purposes. They must also ensure that personal data is adequate, relevant, and limited to what is necessary for the purposes for which it is processed, and that it is accurate and kept up-to-date. Additionally, we shall ensure that personal data is kept secure and confidential, and that it is not transferred without adequate protection.

5. How we collect your information

We collect and process your personal data when you use our services, the following are the instances where we collect your personal data.

The purpose of this policy is to set out the basis on which we will process your personal data,

a. Website and Payment Services: We collect your personal data when you visit and use our website, regardless of where you visit or use them from, and when using our payment services like when you apply for, receive, pay and use any of our services.
b. Communication and Resources: Your personal data is collected when you communicate with us or leave a query, and also when you subscribe to our newsletters or updates.
c. Purpose of collection: The personal data of the users are collected to measure or analyze the website's traffic and the collected information will be shared with the authorized third-parties to provide the services, especially for conducting KYC and AML procedure.

6. Information we collect automatically

Information collected automatically refers to the data that is collected by the website or application without the user explicitly providing it. This data is collected through various means such as cookies, log files, web beacons, and other tracking technologies. This information is used to improve the user experience, provide relevant content, and analyze trends.

When you use our products and services, we may make use of the standard practice of placing tiny data files called cookies, flash cookies, pixel tags, or other tracking tools (herein, "Cookies") on your computer or other devices used when engaging with us.

We use Cookies to (i) help us recognize you as a customer, collect information about your use of our products and services, to better customize our services and content for you, and to collect information about your computer or other access devices to ensure our compliance with our AML obligations.

7. How we use the information we gather

We primarily use the limited information for the following purposes,

a. Service updates: To provide, maintain, debug, and improve our services.
b. Analyze services: To understand and analyze how you use our services and develop new products, services, features, and functionality.
c. Communication and support: To communicate with you, provide you with updates and other information relating to our site and services, provide information that you request, respond to comments and questions, and otherwise provide customer support.

d. Fraud Prevention: To find and prevent fraud, detect security incidents, and respond to trust and safety issues that may arise.
e. Compliance purposes: For enforcing our Terms of Service or other legal rights, or as may be required by applicable laws and regulations or requested by any judicial process or governmental agency.
f. Third party service providers: To contract with third-party API providers, including providing customer service, verifying customer information and to facilitate the connection of third-party services or applications.
g. Other Purposes: For other purposes for which we provide specific notice at the time the Personal Data is collected.

You may be asked to provide personal information anytime you contact our customer support service. We may use your personal information in accordance with this Privacy Policy.

8. How we share the personal data we collect

We do not share or otherwise disclose Personal Data we collect from or about you except as described below or otherwise disclosed to you at the time of collection.

a. Analytics Partners – We use analytics services such as Google Analytics to collect and process certain analytics data. These services also may collect information about your use of other websites and online resources.
b. As required by law and similar disclosures – We may access, preserve, and disclose your personal data if we believe doing so is required or appropriate to:
    i. Comply with applicable laws
    ii. Respond to law enforcement requests and legal process, such as court orders or subpoenas, or
    iii. Protect the rights, property, and safety of Vaultex Wallet, our employees, agents, customers, and others, including to enforce our agreements, policies and Terms of Service.

9. Services provided by third-parties

We may provide information about third-party products, services, activities or events, or may allow third parties to make their content and information available on or through the services (collectively, "Third-Party Integrations").

We provide Third-Party Integrations as a service to those interested in such content. Your dealings or correspondence with third parties and your use of or interaction with any Third-Party Content are solely between you and the third party.

10. Purpose of data processing

a. To provide our services: We process personal data in order to provide our products and services to our users. This includes processing personal data to create user accounts, enabling users to create and share content, providing customer support, and improving our products and services.
b. To communicate with users: We may process personal data to communicate with our users, including responding to their requests, sending newsletters or promotional messages, and providing updates about our products and services.
c. To personalize user experience: We may process personal data to tailor our products and services to individual users' interests, preferences, and usage patterns. This includes analyzing data about user behavior, preferences, and interactions with our products and services.
d. To comply with legal obligations: We may process personal data to comply with legal obligations, such as responding to legal requests or orders, preventing fraud or other illegal activities, and enforcing our terms of service.
e. To improve our products and services: We may process personal data for research and development purposes, including testing new features and functionality, analyzing usage patterns, and improving the quality and performance of our products and services.

11. International data transfers

To facilitate our operations we may transfer, store, and process your information within any country or with the service providers.

Transfers to our affiliated entities, to our service providers and other third parties, will be protected by appropriate safeguards.

We may also share personal data with business partners or other third parties for marketing or advertising purposes, subject to the user's consent where required by law.

We may transfer personal data to international countries outside the jurisdiction where we are based, including to countries that do not provide an adequate level of data protection. In such cases, we will ensure that appropriate safeguards are in place to protect personal data, such as using standard contractual clauses or relying on other legal mechanisms for data transfers.

Users have the right to object to the processing of their personal data for direct marketing purposes and can exercise their other data subject rights as provided.

If you have any questions or concerns about our use of personal data, please contact us at the contact information provided

12. Consent

a. Requirements

Consent is one of the legal bases for processing personal data under this Policy. In order for consent to be valid, it must meet the following requirements:

i. Freely given: Consent must be given voluntarily and without coercion. Users must not be required to give consent in order to access a service, and consent must not be a condition of a contract.
ii. Specific: Consent must be specific to the purpose for which it is given. Users must be informed of the exact purpose for which their data will be processed, and must explicitly agree to that purpose.
iii. Informed: Consent must be informed, meaning users must be provided with clear and understandable information about the processing of their personal data, including the identity of the data controller, the purposes of processing, and any third-party recipients.
iv. Unambiguous: Consent must be unambiguous, meaning it must be given through a clear affirmative action. Pre-ticked boxes or inactivity do not constitute valid consent.
v. Revocable: Users must have the right to withdraw their consent at any time, and withdrawing consent must be as easy as giving it.

b. How consent will be obtained

We will obtain consent from users in a clear and transparent manner, and will ensure that the consent meets the above requirements. We will use the following methods to obtain consent:

i. Opt-in mechanisms: We will use clear and conspicuous opt-in mechanisms, such as checkboxes or buttons, to obtain users' consent.
ii. Granular consent: We will obtain separate and specific consent for each distinct purpose of processing, where appropriate.
iii. Records of consent: We will keep records of users' consent, including the purpose of processing, the method of obtaining consent, and the date and time of consent.
iv. Withdrawal of consent: We will provide users with an easy and accessible way to withdraw their consent, and will honor all requests to withdraw consent in a timely manner.

If you have any questions or concerns about our use of consent or wish to withdraw your consent, please contact us at the contact information provided

13. Your rights to your data

a. Right to Access

This right allows you to obtain confirmation as to whether or not personal data concerning you is being processed by us, and to access a copy of the data. You can request information on the categories of data being processed, the purposes of the processing, any recipients of the data, and the retention periods.

You may also request a copy of the data being processed, which should be provided in a commonly used electronic format.

b. Right to Rectification

If you believe that any of your personal data processed by us is inaccurate or incomplete, you have the right to request that we rectify it. We will take reasonable steps to ensure that any inaccurate data is corrected and that any incomplete data is completed, taking into account the purposes for which it was processed.

c. Right to Erasure

Also known as the "right to be forgotten," this right allows you to request the deletion of your personal data in certain circumstances. This includes situations where the data is no longer necessary for the purposes for which it was collected, when you withdraw your consent for processing, or when you object to the processing of the data. However, there may be legal or other reasons why we need to retain your data, and we will inform you if this is the case.

d. Right to Restrict Processing

In some cases, you may wish to limit the processing of your personal data. This right allows you to request that we restrict the processing of your data in certain circumstances, such as when you contest the accuracy of the data or when you object to the processing of the data. We will continue to store your data, but we will not process it further without your consent, unless it is necessary for legal reasons or to protect the rights of another person.

e. Right to Data Portability

You have the right to obtain a copy of your personal data in a structured, commonly used, and machine-readable format, and to transfer that data to another data controller. This right only applies to data that you have provided to us, and only when the processing is based on your consent or on a contract.

f. Right to Object

You have the right to object to the processing of your personal data in certain circumstances, such as when we are using the data for direct marketing purposes or when we are using it for research or statistical purposes. We will cease processing your data unless we can demonstrate compelling legitimate grounds for the processing, which override your interests, rights, and freedoms, or if the processing is necessary for the establishment, exercise, or defense of legal claims.

g. Right to Withdraw Consent

If we are processing your personal data on the basis of your consent, you have the right to withdraw that consent at any time. This means that we will no longer process your data for the purpose for which you originally gave your consent, unless we have another legal basis for doing so. Withdrawing your consent will not affect the lawfulness of any processing that we have carried out prior to the withdrawal of consent.

14. Security Measures

We have implemented measures designed to secure your personal data from accidental loss and from unauthorized access, use, alteration and disclosure.

We use appropriate technical, organizational and administrative security measures to protect any information we hold in our records from loss, misuse and unauthorized access, disclosure, alteration and destruction. In doing so, we follow any and all regulations and rules established by law to ensure the highest standards of Data Protection.

a. Technical Measures
    i. We use encryption technology to secure personal data during transmission and storage. This includes using SSL/TLS encryption for website traffic and secure connections for remote access.
    ii. We regularly perform vulnerability scans and penetration testing to identify and address security weaknesses.
    iii. We use firewalls, intrusion detection systems, and other network security technologies to protect against unauthorized access or attacks.
    iv. We maintain up-to-date software and hardware to ensure the security of our systems.

b. Organizational Measures
    i. We limit access to personal data to only those employees, contractors, and third parties who require it for legitimate business purposes.
    ii. We provide regular training to our employees on data protection and privacy practice.
    iii. We implement access controls and password policies to ensure that personal data is only accessible to authorized personnel.
    iv. We have established incident response procedures in case of a data breach, and will notify affected individuals and authorities as required by law.

c. Third Party Security Obligations
    i. We require all third-party service providers who process personal data on our behalf to meet the same security standards as we do. This includes requiring them to implement appropriate technical and organizational measures to protect personal data.

ii. We require third-party service providers to provide us with written assurances that they comply with data protection laws and will handle personal data in a manner consistent with our instructions.

d. Incident Response Procedures

The purpose of incident response procedures is to minimize the impact of an incident on us, our customers, and other stakeholders. We have the below mentioned incident response procedures in place that address key components:

i. Detection and Response: The first step in incident response is detecting that a security breach has occurred. We have monitoring systems in place to detect incidents and respond quickly to contain them. This may involve shutting down affected systems or isolating compromised devices to prevent further damage.
ii. Investigation: Once an incident has been detected, we shall conduct a thorough investigation to determine the cause of the incident and the extent of the damage. This may involve reviewing logs, analyzing system activity, and interviewing personnel who were involved.
iii. Notification: If a personal data breach has occurred, we shall notify the relevant supervisory authority and affected data subjects within 72 hours of becoming aware of the breach. Notification shall include a description of the nature of the breach, the types of personal data affected, and the steps being taken to mitigate the impact of the breach.
iv. Mitigation: We shall take steps to mitigate the impact of the incident, such as restoring data from backups, patching vulnerabilities, or implementing additional security controls to prevent similar incidents from occurring in the future.
v. Follow-up: After an incident has been resolved, we shall conduct a post-incident review to identify lessons learned and update incident response procedures as needed.

While we take reasonable steps to protect personal data, no security measure is perfect and we cannot guarantee the absolute security of personal data. In the event of a security breach, we will take all necessary steps to mitigate the impact of the breach and notify affected individuals and authorities as required by law.

15. Information for the visitors based on Jurisdiction

If you are a user who belongs to the following jurisdictions, the rights of the users are provided by the specific laws where you can exercise your rights accordingly.

a. For EEA (European Economic Area) users:

Your rights under the General Data Protection Regulation (GDPR) are:

i. Right to be informed
ii. Right of data portability

iii. Right to access
iv. Right to rectification
v. Right to object to processing
vi. Right to restrict processing
vii. Right to be forgotten
viii. Rights in relation to Automated Decision Making and Profiling

b. For California users:

Your rights under the California Consumer Protection Act (CCPA):

i. Right to Know
ii. Right to Delete
iii. Right to opt-out of sale or sharing
iv. Right to correct
v. Right to limit the use and disclosure of sensitive personal information

c. For U.A.E (“United Arab Emirates”) Users:
Your Rights under Protection of Personal Data Protection (PDPL) are:

i. Right to access to information
ii. Right to request personal data portability
iii. Right to rectification or erasure
iv. Right to restriction of processing
v. Right to stop processing
vi. The right not to be subject to automated decision-making including profiling

d. For United Kingdom users:

Your rights under the Data Protection Act - UK GDPR:

i. Right to access
ii. Right to be informed
iii. Right to rectification, erasure or restriction
iv. Right to object
v. Right to data portability
vi. Right in relation to Automated Decision Making and Profiling

To exercise any of these rights, please contact us using the details provided in the "Redressal and Contact Information" section below. We may need to verify your identity before we can respond to your request. We will respond to your request as soon as possible and in any event within one month of

receipt of your request. However, if your request is complex or if we receive a number of requests from you, we may need to extend this period by a further two months. If we are unable to fulfill your request, we will explain why.

16. Use of Service by Minors

We are especially sensitive about children's information. Our services are not targeted toward children, we do not intend to collect personal data of children or persons under the age of 18 (eighteen) years old.

If you're under the age of 18, please do not attempt to register for the services or send any personal information about yourself to us. If you believe that a child under the age of 18 may have provided us with personal information

17. Data Retention

We retain personal data only for as long as necessary to fulfill the purposes for which it was collected, unless a longer retention period is required by law or our legitimate interests. The retention periods for different types of personal data depend on various factors, including the nature of the data and the purposes for which it was collected. And the retention period as mentioned in the applicable laws will be considered for the retention of the personal data.

a. Retention Periods

We retain personal data for the following periods:

i. Personal data collected for contractual purposes will be retained for the duration of the contract and for a period thereafter as required by applicable law.
ii. Personal data collected for marketing purposes will be retained until you withdraw your consent or until you exercise your right to object.
iii. Personal data collected for compliance with legal obligations will be retained for the period required by the applicable law.

b. Criteria for Determining Retention Periods

We determine the appropriate retention period for personal data based on the following criteria:

i. The purpose for which the personal data was collected.
ii. The nature of personal data.
iii. The legal or regulatory obligations that require us to retain the personal data.
iv. Our legitimate interests in retaining the personal data.

c. Exceptions to Retention Periods

In some circumstances, we may retain personal data for a longer period than stated above if necessary to comply with our legal obligations or to protect our legitimate interests. For example, we may retain personal data for longer periods to resolve disputes, prevent fraud, or enforce our agreements.

If we no longer need personal data for any purpose and are not required by law to retain it, we will securely delete or destroy it in accordance with our data retention and disposal policies.

18. Data Protection Officer

a. Appointment of a DPO
   i. We have appointed a Data Protection Officer (DPO) to ensure compliance with the GDPR and to serve as a point of contact for data subjects and supervisory authorities.
   ii. The DPO's contact information is provided in the Contact Information section of this privacy policy.

b. Role and Responsibilities
   i. The DPO's main responsibilities include:
      - Informing and advising the Company and its employees about their GDPR obligations
      - Monitoring GDPR compliance
      - Providing advice and guidance on data protection impact assessments (DPIAs)
      - Serving as a point of contact for data subjects and supervisory authorities on GDPR-related matters
      - Cooperating with supervisory authorities and acting as a liaison with them on GDPR-related issues
   ii. The DPO reports directly to senior management and operates independently within the organization to ensure that data protection is taken seriously and given appropriate attention.

c. Independence and Resources
   i. The DPO is appointed on the basis of professional qualities, expertise in data protection law, and the ability to fulfill the tasks listed above.
   ii. The DPO is independent and cannot be dismissed or penalized for performing their tasks.
   iii. The organization provides the DPO with the necessary resources to carry out their tasks, including access to personal data and other information, as well as any necessary equipment or support staff.

d. Accountability and Performance
   i. The DPO is accountable to the Company and the supervisory authority for their performance.
   ii. The organization evaluates the DPO's performance on a regular basis and provides them with feedback and support to enable them to carry out their tasks effectively.
   iii. The DPO is responsible for maintaining their knowledge and expertise in data protection law and informing the organization of any developments that may affect its GDPR compliance.

19. Updates to the Privacy Statement

We reserve the right to update and revise the Privacy Policy at any time. We occasionally review this privacy policy to make sure it complies with the applicable laws and confirms changes in our business. If we revise this Privacy Policy, we will update the "Effective Date" at the top of this page and we will do our best to notify you. Please review this Privacy Policy regularly to ensure that you are aware of its terms. Any use of Vaultex Wallet after an amendment to our Privacy Policy constitutes your acceptance to the revised or amended terms.

20. Redressal and Contact Information

a. Complaints Procedure
   i. We take all complaints about our handling of personal data seriously and are committed to addressing them promptly and effectively.
   ii. Data subjects can submit a complaint about our data handling practices by contacting us using the information provided in the Contact Information section of this Privacy Policy.
   iii. We will acknowledge receipt of the complaint and provide the data subject with a reference number for tracking purposes.

b. Investigation and Resolution
   i. We will investigate the complaint promptly and thoroughly, taking into account all relevant circumstances and any applicable legal requirements.
   ii. We may request additional information or documentation from the data subject or any third parties involved in order to assist with the investigation.
   iii. We will notify the data subject of the outcome of the investigation and any remedial action taken as a result of the complaint.

c. Timeframes: We aim to respond to all complaints within 30 days of receipt. However, in some cases, we may require additional time to investigate the complaint fully. In such cases, we will notify the data subject of the reason for the delay and provide an estimated timeframe for resolution.

d. No Retaliation
   i. We will not retaliate against any data subject for submitting a complaint about our data handling practices.
   ii. We will take appropriate measures to prevent any retaliation by employees, service providers or contractors against data subjects who submit a complaint.

We respect the personal data and privacy of every user equally, irrespective of their jurisdiction. We promise to abide by this Privacy Statement and secure your privacy. For us, you all are equally valuable, and your trust is our asset. If you have any questions, comments, or concerns about this notice or our processing activities, or you would like to exercise your privacy rights, please email us contact@wafee.co.