Privacy Policy

Last Updated: 04.09.2026

This Privacy Policy ("**Policy**") describes how Ostrand Ltd, a company incorporated and registered under the laws of the Republic of Seychelles under registration number 251987, having its registered office at 306 Victoria House, Victoria, Mahe, Seychelles ("**we**," "**us**," or "**the Company**") collects, uses, stores, and protects personal data in connection with your use of B2BWALLET, together with its website, personal dashboard, API, and other interfaces through which the Service may be made available (collectively, the "**Service**").

By registering an Account, generating an API Key, or otherwise accessing or using the Service, you acknowledge that you have read, understood, and accept this Policy. If you do not agree with this Policy, you must discontinue use of the Service immediately.

1. General Provisions

1.1. This Privacy Policy sets out the principles governing the collection, use, storage, disclosure, and protection of personal data processed in connection with the operation of the Service.

1.2. The Company processes two broad categories of data:

- **Off-Chain Data** - data we or our service providers hold on our own systems, such as your email, password, identity-verification documents, IP address, and support communications.
- **On-Chain Data** - information recorded on the relevant public blockchain network when a Transaction is executed, such as wallet addresses, transaction amounts, and transaction hashes. Depending on the circumstances, such information may be capable of being associated with an identifiable User. On-Chain Data is publicly and permanently recorded on the relevant blockchain network once a Transaction is confirmed. This data cannot be altered or deleted, including by us, and may be accessible to anyone with internet access.

1.3. The Company is committed to ensuring that personal data is processed lawfully, fairly, and transparently, and only to the extent necessary for legitimate business and operational purposes, including compliance with applicable AML/KYC requirements.

1.4. The Service is not intended for individuals under 18. We do not knowingly collect personal data from anyone under 18. By using the Service, you confirm that you are at least 18 years old. If we become aware that an Account belongs to a person under 18, we will request closure of the Account and delete the associated personal data from our systems, to the extent permitted by our legal recordkeeping obligations. If you are a parent or guardian and believe a minor has shared personal data with us, contact us at support@b2bwallet.io.

1.5. We do not collect or process data relating to race, political opinions, religious beliefs, or membership of political or social organizations.

2. Data Collection

2.1. This section sets out the categories of Off-Chain Data we process, why we process them, and the legal basis for doing so.

2.2. We collect and process only such personal data as is necessary for the provision of the Service and compliance with applicable legal obligations. Categories of Processed Data:

- **Account & Registration Data** - email address, password (encrypted), account type, and, for Partners, corporate details and authorized representatives. Processed to create and administer your Account, on the basis of Performance of a Contract.
- **Identity Verification (AML/KYC) Data** - information and documents required to verify your identity and comply with applicable AML/CFT and other legal requirements, which may include your full name, date of birth, identity document, proof of address, and other information or documents requested under our AML/KYC Policy. Processed for compliance with applicable legal and regulatory obligations.
- **Security & Authentication Data** - login credentials, 2FA codes, login timestamps, IP address, device/browser data, and, for Partners, API Keys. Processed to secure your Account and API access and detect unauthorized activity, on the basis of Performance of a Contract and Legitimate Interests.
- **Transaction Data** - wallet addresses, amounts, fees, Transaction status, transaction hash, and any labels you assign. Processed to execute your Transactions and maintain your history, on the basis of Performance of a Contract.
- **Partner / API Data** - API Key, callback URL, and request logs. Processed to authenticate API requests and deliver Transaction callbacks, on the basis of Performance of a Contract.
- **Referral Program Data** - referral link ID, the association between referring and referred Accounts, and partnership balance. Processed to administer the Referral Program and calculate rewards, on the basis of Performance of a Contract.
- **Support Communications** - your Account email or ID, wallet address, message content, and technical data collected by our support channel. Processed to resolve inquiries and disputes, on the basis of Legitimate Interests.
- **Website Usage Data** - IP address, browser type, pages visited, and cookie identifiers. Processed to operate and secure the Website, on the basis of Legitimate Interests and, for non-essential cookies, Consent.

2.3. In certain cases, we may also obtain data indirectly from third parties, including but not limited to:

- from public blockchain networks, in connection with deposits, withdrawals, and conversions;
- from identity-verification service providers, in connection with AML/KYC checks;
- from infrastructure or analytics service providers supporting the operation of the Service.

2.4. To ensure the proper functioning, security, and performance of the Service, we may use cookies and similar technologies, which may collect limited technical data as described further in Section 4.

2.5. We may also process personal data contained in your communications, feedback, or support requests submitted to us via email, Telegram, or other official channels.

3. Data Usage

3.1. The legal grounds for processing personal data include:

- **Consent**, where required by applicable law, for specific processing activities that are not necessary for the performance of the Service or compliance with legal obligations;
- **Performance of a contract**, processing is necessary to provide the Service, including account management, notifications, and User support;
- **Compliance and legal obligations**, ensuring adherence to legal and regulatory requirements, including AML/KYC and cooperation with competent authorities;
- **Legitimate interests**, improving the Service, monitoring platform performance, ensuring security, and preventing fraud.

3.2. We process personal data primarily to provide, operate, and improve the Service, and to comply with applicable legal obligations. This includes the following purposes:

- **Account management** - registration, authentication, and maintenance of your Account;
- **Wallet and Transaction Operations** - processing deposits, withdrawals, and conversions, and maintaining your Transaction history;
- **API access** - authenticating requests made with your API Key and delivering Transaction callbacks;
- **Referral Program** - attributing referrals and calculating rewards;
- **Notifications and communication** - sending Service-related notifications via email or other channels made available through the Service;
- **User support** - responding to inquiries and resolving issues related to your Account or Transactions;
- **Service monitoring, security and analytics** - monitoring platform performance, detecting errors, preventing fraud and unauthorized access, maintaining security, and improving the Service;

3.3. We do not use personal data for marketing or advertising profiling.

3.4. You retain control over your personal data and may update, correct, or request deletion of account information in accordance with Section 8.

4. Cookies and Related Technologies

4.1. The Website uses cookies and similar technologies to operate core functions, remember your preferences, and understand how the Website is used.

4.2. Cookies are small data files stored on your device that allow the Service to recognize sessions, maintain authentication, and support certain platform features. Cookies and similar technologies may be associated with technical identifiers and other information relating to the device or browser used to access the Service.

4.3. The Service may use several categories of cookies and similar technologies:

- **Essential cookies** - required for login sessions, security, and core functionality (e.g., session tokens, authentication state). These are deleted upon logout or when your session expires;
- **Preference and functional cookies** - remember your interface preferences, such as your selected language and display currency, and support certain functionality of the Service. Retained for up to [12] months.

4.4. In addition to cookies, the Service may collect **usage and activity data** generated when you interact with the platform. Such data may include navigation within the Service, interaction with interface elements, records of actions performed within the platform, and operational activity associated with your account.
4.5. This information is used for purposes such as operation and maintenance of the Service, security monitoring and fraud prevention, internal analytics and performance monitoring, customer relationship management, improvement of platform functionality and your experience.
4.6. The Service may use internal analytics systems or third-party monitoring tools that automatically collect technical and usage information, including device type, browser type, operating system, pages visited, interaction logs, and diagnostic data. Where third-party analytics providers are used, the processing of data by such providers is governed by their respective privacy policies.
4.7. Certain cookies and activity tracking technologies are necessary for the operation, security, and functionality of the Service. These technologies cannot be disabled without affecting the availability or proper functioning of the platform.
4.8. Where required by applicable law, the Service will request your consent before placing or using certain categories of cookies or tracking technologies.
4.9. We do not currently use cookies for advertising or remarketing purposes.

5. Data Sharing

5.1. The Company does not sell personal data or disclose personal data to third parties for their own independent marketing purposes.
5.2. Access to your data is limited to team members who need it to perform their role (e.g., compliance, support, engineering), subject to confidentiality obligations and role-based access controls.
5.3. We may disclose your data where we believe in good faith this is necessary to:

- comply with applicable law or a legitimate order from a competent court, regulator, or law enforcement authority;
- enforce our Terms of Use or investigate a suspected violation;
- prevent or investigate fraud, money laundering, terrorist financing, sanctions evasion, or other unlawful activity; or
- protect the security and integrity of the Service.

5.4. We may engage third-party service providers to process personal data on our behalf for purposes such as identity verification, cloud hosting, infrastructure, cybersecurity, analytics, customer support, communications, and payment processing. Such service providers are permitted to process personal data only as necessary to provide the relevant services and in accordance with applicable contractual and legal requirements.
5.5. Personal data may be processed or stored by the Company and its service providers in jurisdictions outside your country of residence. Where required by applicable law, the Company will implement appropriate safeguards for such transfers and processing.

6. Data Retention

6.1. We do not retain Off-Chain Data longer than necessary for the purposes described in this Policy or as required by applicable law.

6.2. Retention periods by category:

- **Account information** - retained for the duration of active use of your Account.
- **Identity-verification (AML/KYC) data** - retained for 5 years following Account closure, in line with applicable AML/CFT recordkeeping obligations.
- **API Keys and request logs** - retained encrypted until the API Key is revoked or the Account is deleted.
- **Transaction data** - retained for 5 years for accounting, audit, and legal compliance purposes.
- **Referral Program data** - retained for the duration of your participation and [1] year thereafter.
- **Security and access logs** - retained for [30–90] days for fraud prevention and security monitoring.
- **Support communications** - retained for [12] months after resolution, or longer if related to an unresolved dispute.
- **Cookies** - retained per the periods disclosed at the point of collection.

6.3. **On-Chain Data** is permanent and immutable, as described in Section 1, and is not subject to our retention or deletion schedules.

7. Data Security

7.1. We apply technical and organizational safeguards appropriate to the sensitivity of the data we process, including:

- Encryption of API Keys, passwords, and other sensitive data at rest;
- Access controls, limiting internal access to personal data on a role-based basis;
- 2FA, applied to Account logins and sensitive operations;
- Monitoring, to detect and respond to unauthorized activity.

7.2. **Disclaimer**. No method of transmission or storage is completely secure, and we cannot guarantee the absolute security of the data we process. You are responsible for safeguarding your own Credentials, 2FA method, and API Keys, as set out in our Terms of Use.

8. Data Protection Rights

8.1. Depending on your location, you may have the following rights over your Off-Chain Data:

- **Right of access** - request confirmation of, and access to, the data we hold about you;
- **Right to rectification** - request correction of inaccurate or outdated data;
- **Right to erasure** - request deletion of your data, subject to our legal retention obligations (in particular, AML/KYC and transaction recordkeeping);
- **Right to object / restriction** - object to processing based on legitimate interests, or request that we restrict it;
- **Right to data portability** - where applicable, request your data in a structured, commonly used format;

- **Right to withdraw consent** - where processing is based on your consent, you may withdraw such consent at any time, without affecting the lawfulness of processing carried out before its withdrawal.

8.2. **Limitations on On-Chain Data**. Due to the decentralized and immutable nature of public blockchain networks, the Company generally cannot modify or delete information that has already been recorded on-chain. Accordingly, certain data protection rights may not be capable of being exercised in relation to such information.

8.3. **Exercising Your Rights**. Contact us at support@b2bwallet.io. We may need to verify your identity before processing your request, including confirming ownership of your registered email address or Account.

8.4. **Right to Lodge a Complaint**. You may lodge a complaint with the data protection authority in your country of residence if you believe your rights have been violated.

9. Concluding Provisions

9.1. We may update this Policy at any time to reflect changes in legal requirements, our data processing practices, or the Service itself. Where changes are material - such as new categories of data, new third-party processors, or changed retention periods - we will notify you through the Service or by email. Continued use of the Service after such changes take effect constitutes your acceptance of the updated Policy.

9.2. Where a data breach is likely to pose a high risk to your rights and freedoms, we will notify you where feasible and inform the relevant supervisory authority as required by applicable law.

9.3. This Policy is governed by the laws of the Republic of Seychelles, without regard to conflict-of-law principles, unless mandatory provisions of your local jurisdiction require otherwise. You agree to first attempt to resolve any dispute by submitting a written complaint to support@b2bwallet.io; we will respond within 30 calendar days. Unresolved disputes are subject to the exclusive jurisdiction of the courts of the Republic of Seychelles. Any claim must be brought within one (1) year of the date it arose.

9.4. For questions about this Policy or to exercise your data rights, contact us at support@b2bwallet.io or via our official Telegram support channel @b2bwallet_support.