

## PRIVACY POLICY

Last Updated: February 05, 2026

### SUMMARY OF KEY POINTS

*(This summary highlights key points. Please read the full policy for details.)*

**What personal information do we process?** We only process minimal information necessary for Wallet App functionality and compliance (e.g., device identifiers for notifications, technical and usage information). Your cryptographic keys, assets, and transaction information are processed only on your own device and are never sent to us. [\[See Section 1\]](#).

**Do we process any sensitive personal information?** We do not process any sensitive personal information. [\[See Section 1\]](#)

**Do we receive any information from third parties?** We do not receive any personal information about you from third parties. The Wallet App displays public information from the blockchain on your device only. We never receive or store this data. [\[See Section 1\]](#)

**How do we process your information?** We process your information to provide and maintain the functionality of the Wallet App, to improve its performance, and to comply with applicable laws. We do not use your data for marketing, profiling, or any purpose not disclosed to you [\[See Section 2\]](#).

**In what situations and with which parties do we share personal information?** We only share data with essential service providers under contract (e.g. push notification services or analytics platforms) or when required by law. All transfers are governed by strict contracts and safeguards. [\[See Section 4\]](#).

**How do we keep your information safe?** We have implemented strong organizational and technical measures to protect your personal information. [\[See Section 7\]](#).

**What are your rights?** Depending on your location, you have certain rights over your personal information. Your rights are linked to the specific, limited data we process. For data we cannot link to you (such as anonymized analytics or session-only data), certain rights like access may not be possible. For data we can link to your device (like a push notification token), your rights can be exercised as described in Section 9. [\[See Section 9\]](#).

**How do you exercise your rights?** The easiest way to exercise your rights is by using the settings within the Wallet App or by contacting us at [privacy@outbe.app](mailto:privacy@outbe.app). [\[See Section 9\]](#).

Want to learn more about what we do with any information we process? Review the Policy [in full below](#).

## **TABLE OF CONTENTS**

<b>PRIVACY POLICY</b>	<b>1</b>
SUMMARY OF KEY POINTS	1
INTRODUCTION & SCOPE	4
1. WHAT INFORMATION DO WE PROCESS?	5
2. HOW DO WE PROCESS YOUR INFORMATION?	6
3. WHAT LEGAL BASES DO WE RELY ON TO PROCESS YOUR INFORMATION?	6
4. WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?	7
5. IS YOUR INFORMATION TRANSFERRED INTERNATIONALLY?	8
6. HOW LONG DO WE KEEP YOUR INFORMATION?	8
7. HOW DO WE KEEP YOUR INFORMATION SAFE?	9
8. DO WE PROCESS INFORMATION FROM MINORS?	10
9. WHAT ARE YOUR PRIVACY RIGHTS?	10
10. CONTROLS FOR DO-NOT-TRACK FEATURES	12
11. DO UNITED STATES RESIDENTS HAVE SPECIFIC PRIVACY RIGHTS?	12
12. DO WE MAKE UPDATES TO THIS POLICY?	15
13. INFORMATION YOU PROVIDE IN DIRECT COMMUNICATIONS	15
14. HOW CAN YOU CONTACT US ABOUT THIS POLICY?	16

## INTRODUCTION & SCOPE

This Policy describes how **outbe App US Inc.** (“Wallet Provider,” “we,” “us,” or “our”) processes your personal information when you use the **outbe App** wallet application (“Wallet App”).

The Wallet App operates as a non-custodial digital wallet, providing you with exclusive control over your cryptographic private keys and digital assets. The Wallet App serves as an interface to:

- (a) Manage digital assets on various blockchain networks.
- (b) Interact with the outbe Network ecosystem.
- (c) Access third-party services (each governed by their own terms of use and privacy policies).

**Important:** We do not have access to, visibility into, or control over your cryptographic private keys or the digital assets they control. The Wallet App acts purely as a user-side interface. It does not perform, intermediate, or store any blockchain or banking transactions. **You are solely responsible for the security of your private keys and recovery phrases.** Losing them will result in the permanent loss of access to your digital assets.

**Scope:** This Policy applies when you download and use our Wallet App or engage with us in other related ways. This Policy covers only the limited technical information processed by the Wallet Provider in providing the Wallet App. Any financial data needed by the outbe Network protocol is processed by independent third parties (Consumption Reflection Agents, “CRAs”). You will enter into a separate agreement directly with a CRA, and your data will be governed exclusively by that CRA's terms and privacy policy. **Wallet Provider is not a party to those agreements and does not receive or control any financial data.**

**Data Controller:** Wallet Provider acts as the data controller for the information described in this Policy.

**Jurisdiction:** This Policy applies worldwide to all users of the Wallet App. We comply with applicable data protection laws in the jurisdictions where we operate, including but not limited to various United States privacy laws, the EU General Data Protection Regulation (GDPR), and the UK GDPR.

**Questions or concerns?** Reading this Policy will help you understand your privacy rights and choices. If you do not agree with our policies and practices, please do not use the Wallet App. If you have questions or concerns, please contact us at [privacy@outbe.app](mailto:privacy@outbe.app).

## 1. WHAT INFORMATION DO WE PROCESS?

**In Short:** We process minimal personal information required for the Wallet App functionality and compliance. We do not obtain any personal information from third-party sources; all information we process is provided by you through your use of the Wallet App.

### Categories of Information Processed:

Category	Description	Our Access
Wallet Information	Public wallet address and wallet private keys <i>*This information is stored locally on your device under your custody</i>	None - processed locally on device
Transaction Information	Public digital asset balances and transaction history (e.g., sender/receiver addresses, amounts)	None - processed locally on device
Device Identifier	Push notification token (only if you opt-in)	None - not linked to identity

### Information automatically collected:

**Technical and Usage Information:** To maintain the functionality of our Wallet App, we automatically process a limited set of technical and usage information. This information is processed in a way that does not identify you personally and includes:

- (a) **Device Information:** We collect your device type (e.g., “iPhone 17”) and operating system version (e.g., “iOS 26.0.1”) to ensure app compatibility, deliver updates, and provide effective technical support.
- (b) **Anonymized Usage Analytics:** We process anonymized and aggregated interaction information (e.g., which features are most used, screen view counts) to identify bugs and improve the user experience.

### Information we do NOT collect or access:

- (a) Private keys (generated and stored exclusively on your device)
- (b) Personal identity information
- (c) Payment card details
- (d) Biometric data
- (e) Financial data from banks or CRAs

**Sensitive Information:** We do not process sensitive information.

## 2. HOW DO WE PROCESS YOUR INFORMATION?

***In Short:** We process your information to provide and maintain the functionality of the Wallet App, to improve its performance, and to comply with applicable laws.*

We process your personal information to:

- (a) **Provide and maintain Wallet App functionality:** We process minimal information to operate the Wallet App, ensure compatibility across devices, and enable blockchain information display.
- (b) **Connect with ecosystem services:** The Wallet App facilitates direct connections to CRAs and other outbe Network components.
- (c) **Comply with legal obligations:** We may process limited information when required by applicable law, regulation, or court order.
- (d) **Fulfill other purposes with your consent:** Any additional processing purposes will be clearly communicated at the time of collection and will occur only with your explicit consent.

We do not process your personal information for marketing purposes and do not use automated decision-making, including profiling, that produces legal effects concerning you or similarly significantly affects you.

## 3. WHAT LEGAL BASES DO WE RELY ON TO PROCESS YOUR INFORMATION?

***In Short:** We process your personal information only when we have a valid legal basis under applicable law.*

***If you are located in the EU or UK, this section applies to you.***

The EU GDPR and the UK GDPR require us to explain the valid legal bases we rely on to process your personal information:

- (a) **Consent:** We may process your information if you have given us permission (i.e., consent) to use your personal information for a specific purpose. You can withdraw your consent at any time through the Wallet App settings.
- (b) **Contract performance:** Once you accept our Terms of Use, we process your personal information as necessary to perform our contractual obligations and provide the Wallet App functionality in accordance with those Terms.
- (c) **Legitimate Interests:** We may process your information when we believe it is reasonably necessary to achieve our legitimate business interests and those interests do not

outweigh your interests and fundamental rights and freedoms. For example, we may process your personal information for some of the purposes described in order to analyze how our Wallet App is used so we can improve it, or diagnose problems.

- (d) **Legal Obligations:** We may be required to process data to comply with applicable laws and regulations, or valid requests from supervisory authorities. However, due to our non-custodial architecture, our ability to provide data is limited.

**Legal Basis Framework:** The table below specifies our legal basis for each processing activity:

Processing Activity	Personal Information Categories	Legal Basis
Display of Wallet & Transaction Information	Wallet & Transaction Information. Not processed by us (device-only)	Contract Performance
Push Notifications	Device Identifier	Explicit Consent
Provide and Maintain the Wallet App Functionality	Device Information	Contract Performance
Service improvement	Anonymized Usage Analytics	Legitimate Interest
Responding to Lawful Requests	Technical or communication information	Legal Obligation

#### 4. WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?

**In Short:** We may share information only with our direct service providers, when required by law, or with your consent.

We may share your personal information in the following situations:

- (a) **With service providers acting on our behalf:** We share information only with our contracted service providers (or "processors") who perform services on our behalf. Push notification services receive device tokens solely for message delivery purposes. Analytics providers receive only aggregated information data. These providers cannot access the content of your Wallet App or any other personal information. They must process the personal information in accordance with our contractual agreements and only as permitted by applicable data protections laws.
- (b) **Legal Compliance and Law Enforcement:** We may need to comply with applicable laws, regulations, or valid legal requests from supervisory authorities, courts, or law enforcement. Given our minimal data processing, such disclosures would typically be limited to technical information.

- (c) **With your consent:** We may share your personal information for any other purposes disclosed to you at the time of collection with your explicit consent.

The Wallet App acts as an interface that allows you to connect with independent third-party services, such as CRAs and dApps. These services are independent data controllers. Any information you choose to share with them is provided directly by you and is governed exclusively by their privacy policies. We are not responsible for the privacy practices of any third party.

## 5. IS YOUR INFORMATION TRANSFERRED INTERNATIONALLY?

*In Short:* We may transfer and process your information in countries other than your own.

We maintain infrastructure through trusted service providers, and your information may be processed on servers located outside of your country of residence, primarily in the United States where our company is based.

Where we process your personal information outside your country of residence, we implement appropriate technical, organizational, and contractual safeguards to ensure your information remains protected. For transfers from the European Economic Area and United Kingdom, we rely on Standard Contractual Clauses. For transfers from other jurisdictions, we implement comparable safeguards as required by local law. These measures ensure that any transfers comply with applicable data protection laws and maintain an adequate level of protection for your personal information as outlined in this Policy.

For transparency, you may request information about our specific safeguards for international transfers by contacting us at [privacy@outbe.app](mailto:privacy@outbe.app).

## 6. HOW LONG DO WE KEEP YOUR INFORMATION?

*In Short:* We keep your information for as long as necessary to fulfill the purposes outlined in this Policy.

### Data Retention Framework:

Data Type	Retention Period	Purpose
Wallet Information	Never stored by us (device-only)	N/A
Transaction Information	Never stored by us (device-only)	N/A

<b>Data Type</b>	<b>Retention Period</b>	<b>Purpose</b>
Device Identifier	While push notifications are enabled	Notification delivery
Device Information	While the Wallet App is installed	Wallet App compatibility, updates, and technical support
Anonymous Usage Analytics	Aggregated immediately upon collection	Service improvement

## **7. HOW DO WE KEEP YOUR INFORMATION SAFE?**

***In Short:** We implement organizational and technical security measures to protect your personal information.*

We have implemented appropriate and reasonable technical and organizational security measures designed to protect the limited personal information we process. Our security framework is built upon the core principles of non-custodial design and data minimization. This architecture ensures your private keys are generated and stored exclusively on your device and never leave it. To protect the minimal data we handle, all data transmissions are encrypted using industry-standard protocols. Access to this information is governed by our internal security policies and standards, which enforce strict access controls on a need-to-know basis.

However, no electronic transmission over the Internet or information storage technology can be guaranteed to be 100% secure. Therefore, any transmission of personal information to and from the Wallet App is at your own risk, and you should only access the Wallet App within a secure environment.

In the event of a personal data breach affecting your personal information, we will notify affected individuals and applicable supervisory authorities as required by law.

As a user of a non-custodial wallet, you are solely responsible for the security of your cryptographic private keys and recovery phrases. We never have access to your keys and cannot assist you with account recovery.

We regularly review our security practices and may engage third-party security auditors to assess our systems.

## 8. DO WE PROCESS INFORMATION FROM MINORS?

*In Short: We do not knowingly process data from or market to individuals under 18 years of age.*

Our Services are intended only for individuals who are at least 18 years old. We do not knowingly process data from individuals under 18 years of age, nor do we knowingly sell such personal information. By using the Wallet App, you represent that you are at least 18 years old.

Parents and guardians are responsible for monitoring and controlling access to wallet applications on devices accessible to minors. If you have questions concerning our information practices with respect to children, or if you learn that an individual under the age of 18 has used the Wallet App, or provided us with personal information, contact us.

Upon receiving such notification, especially concerning a child under 13 in accordance with the Children's Online Privacy Protection Act (COPPA), we will use the provided information only to respond and inform the individual that they cannot use the Wallet App. We will then take reasonable measures to promptly delete that information from our records.

## 9. WHAT ARE YOUR PRIVACY RIGHTS?

*In Short: You have rights that allow you greater access to and control over your personal information.*

**Your Rights Under Data Protection Laws:** In some regions (like the EEA, UK, and Switzerland), you have certain rights under applicable data protection laws. These may include the right:

- (a) to request access and obtain a copy of your personal information
- (b) to request rectification or erasure
- (c) to restrict the processing of your personal information
- (d) if applicable, to data portability
- (e) not to be subject to automated decision-making
- (f) to object to the processing of your personal information.

**Important Note:** Our ability to fulfill your rights depends on the specific personal information involved. Our non-custodial design means we cannot access, identify, or control any personal information stored only on your device (such as your private keys or transaction history) or on public blockchains. For the limited technical information we do process:

- (a) **Unidentifiable Information:** For information that is not linked to you, such as aggregated analytics, we cannot fulfill rights of access, rectification, or erasure because we are unable to identify you from this data. This is in accordance with GDPR Article 11(2).
- (b) **Identifiable Information:** You have full rights over the data we can link to your device, such as your Device Identifier for push notifications. You can exercise these rights as described in the table below.

**How to Exercise Your Rights:**

<b>Right</b>	<b>Applicability/Status</b>	<b>How to Exercise</b>
Right to Withdraw Consent	<b>Available.</b> Applies to Push Notifications, which are based on your consent.	You may withdraw your consent at any time by disabling push notifications in the Wallet App's settings.
Right to Object	<b>Available.</b> Applies to processing based on our Legitimate Interests (i.e., service improvement analytics).	You may object to our processing of analytics data by disabling "Usage Analytics" in the Wallet App's settings.
Right to Access	<b>Limited.</b> You may request a copy of the identifiable information we hold (e.g., your push notification token).	Contact us at <a href="mailto:privacy@outbe.app">privacy@outbe.app</a> . We cannot provide access to data we cannot identify (per Art. 11(2)) or data on your device.
Right to Erasure (Deletion)	<b>User-controlled.</b> You can erase all app-related technical information at any time.	You can erase your information by uninstalling the Wallet App from your device
Right to Portability	<b>User-controlled.</b> We do not store your on-chain assets or keys.	Your private keys, which remain on your device, enable full portability of your blockchain assets to any compatible wallet.
Right to Rectification	<b>Not applicable.</b> We do not process identifiable information that is user-editable or subject to inaccuracy (e.g., we do not	N/A

Right	Applicability/Status	How to Exercise
	have your name or email).	

**Withdrawing your consent:** You have the right to withdraw your consent for data processing at any time. To withdraw consent, please use the tools provided by your Wallet App.

**Complaints to Data Protection Authorities:** While we encourage you to contact us first at [privacy@outbe.app](mailto:privacy@outbe.app) so we can try to address your concerns directly, you retain the right to file a complaint with your local data protection authority regarding our privacy practices.

If you are located in the EEA or UK and you believe we are unlawfully processing your personal information, you also have the right to complain to your local data protection authority:

- **EEA residents:** Contact your Member State data protection authority. A list of EEA authorities is available from the European Data Protection Board (EDPB) [here](#).
- **UK residents:** Contact the Information Commissioner's Office (ICO) [here](#).
- **Other locations:** contact your local data protection authority.

**10. CONTROLS FOR DO-NOT-TRACK FEATURES**

**Cookies and Tracking Technologies:** Our Services do not use cookies, pixels, web beacons, local storage, or similar tracking technologies. We do not track your browsing activity, and we do not collect any information about your device, browser, or online behavior. Because we do not use these technologies, there are no cookie preferences for you to manage.

Most web browsers and some mobile operating systems and mobile applications include a Do-Not-Track (“DNT”) or Global Privacy Control ('GPC') feature or setting you can activate to signal your privacy preference not to have data about your online browsing activities monitored and collected.

Since we do not engage in tracking or collect browsing data, these signals do not affect our data processing. At this stage, no uniform technology standard for recognizing and implementing DNT signals has been finalized. As such, we do not currently respond to DNT browser signals or any other mechanism that automatically communicates your choice not to be tracked online.

Because our Wallet App does not track you, sell your personal information, or “share” your personal information for cross-context behavioral advertising, we honor “Do Not Sell or Share” preference signals, such as the Global Privacy Control (GPC), by default, as there is no such activity from which to opt you out.

## 11. DO UNITED STATES RESIDENTS HAVE SPECIFIC PRIVACY RIGHTS?

**In Short:** *If you are a resident of a US state with a comprehensive privacy law (such as California, Colorado, Virginia, and others), you have specific privacy rights. More information is provided below.*

**Categories of Personal Information We Process:** U.S. state privacy laws, such as the California Consumer Privacy Act (CCPA), the Colorado Privacy Act (CPA), the Connecticut Data Privacy Act (CTDPA), the Virginia Consumer Data Protection Act (VCDPA), and similar laws in other states, require us to provide additional information about the categories of personal information we process. The following table details the categories of personal information we have collected and processed in the preceding 12 months.

CCPA Category	Personal Information We Process	Purpose of Processing	Disclosed to Service Providers?	Sold or Shared?
A. Identifiers	Device Identifier (if push notifications are enabled)	To provide push notifications.	Yes. Device Identifier is disclosed to our push notification provider.	No
F. Internet or other similar network activity	Device Information (e.g., OS version); Anonymized Usage Analytics	To ensure Wallet App compatibility, deliver updates, and improve user experience.	Yes. Device Information is disclosed to our analytics and diagnostics providers.	No

We may also process other personal information (such as Identifiers (email address)) when you send inquiries to our general privacy email address, as described in [Section 13](#).

**Retention:** We retain personal information in accordance with [Section 6](#).

**Sources of Personal Information:** Learn more about the sources of personal information we process in [Section 1](#).

**How We Use and Share Personal Information:** Learn more about how we use your personal information in [Section 2](#) and how we disclose personal information in [Section 4](#).

### Your Rights Under U.S. State Privacy Laws

**Notice of Sale/Sharing Practices:** We do not and will not "sell" or "share" your personal information

as those terms are defined under California law or under any other applicable U.S. state privacy law.

**Right to Limit Use of Sensitive Personal Information:** We do not collect or process any Sensitive Personal Information. Therefore, a "Right to Limit" is not applicable.

**Your Rights:** You have rights under certain US state data protection laws. However, these rights are not absolute, and in certain cases, we may decline your request as permitted by law. Due to our privacy-focused design, we may be unable to fulfill certain requests as we cannot identify individual users. These rights include:

- Right to know whether or not we are processing your personal information
- Right to access your personal information
- Right to correct inaccuracies in your personal information
- Right to request the deletion of your personal information
- Right to obtain a copy of the personal information you previously shared with us
- Right to non-discrimination for exercising your rights
- Right to opt out of the processing of your personal information if it is used for targeted advertising (or sharing as defined under California's privacy law), the sale of personal information, or profiling in furtherance of decisions that produce legal or similarly significant effects ("profiling").

We do not engage in targeted advertising, sale of personal information, or such profiling. Therefore, an opt-out right is not applicable.

Depending upon the state where you live, you may also have the following rights:

- Right to access the categories of personal information being processed (as permitted by applicable law, including the privacy law in Minnesota)
- Right to obtain a list of the categories of third parties to which we have disclosed personal information (as permitted by applicable law, including the privacy law in California, Delaware, and Maryland)
- Right to obtain a list of specific third parties to which we have disclosed personal information (as permitted by applicable law, including the privacy law in Minnesota and Oregon)
- Right to review, understand, question, and correct how personal information has been profiled (as permitted by applicable law, including the privacy law in Minnesota)
- Right to limit use and disclosure of sensitive personal information (as permitted by applicable law, including the privacy law in California)
- Right to opt out of the collection of sensitive data and personal information collected through the operation of a voice or facial recognition feature (as permitted by applicable law, including the privacy law in Florida)

**How to Exercise Your Rights:** To exercise these rights, you can contact us by emailing us at [privacy@outbe.app](mailto:privacy@outbe.app), or by referring to the contact details at the bottom of this document.

**Appeals:** Under certain US state data protection laws, if we decline to take action regarding your request, you may appeal our decision by emailing us at [privacy@outbe.app](mailto:privacy@outbe.app). We will provide a written response within 45 days (or 60 days where permitted by applicable law) explaining our reasoning. If your appeal is denied, our response will also explain how you can contact your state Attorney General to file a complaint.

**California “Shine The Light” Law:** California Civil Code Section 1798.83 permits California residents to request information about categories of personal information disclosed to third parties for direct marketing purposes. We do not disclose personal information to third parties for direct marketing. Submit requests to [privacy@outbe.app](mailto:privacy@outbe.app).

## 12. DO WE MAKE UPDATES TO THIS POLICY?

*In Short:* Yes, we will update this Policy as necessary to stay compliant with relevant laws.

We may update this Policy from time to time. The updated version will be indicated by an updated “Last Updated” date at the top of this Policy. If we make material changes, we will notify you at least 30 days before the changes take effect by prominently posting a notice through the Wallet App. We encourage you to review this Policy frequently to be informed of how we are protecting your information.

## 13. INFORMATION YOU PROVIDE IN DIRECT COMMUNICATIONS

When you contact us directly via our privacy email address, [privacy@outbe.app](mailto:privacy@outbe.app), we process the personal information you provide to us. This processing is separate from the data processing that occurs when you use the Wallet App and is governed by different rules as described below:

- (a) **Categories of Information Processed:** We process your email address, your name (if provided), and any other personal information contained in the body of your correspondence.
- (b) **Purpose of Processing:** We process this information for the sole purpose of responding to your inquiries, providing you with information about our policies, and managing our legal and regulatory compliance communications.
- (c) **Legal Basis (for EEA/UK residents):** We process this information based on our legitimate interests to manage and respond to user communications and to ensure our legal compliance.

- (d) **Retention:** We retain this correspondence only for as long as necessary to resolve your inquiry and for a limited period thereafter as may be required to comply with our legal obligations or for record-keeping purposes.
- (e) **Your Privacy Rights:** You retain your full data subject rights with respect to this specific information. Because we can identify you by your email address, you may exercise your rights to access, rectify, or request the erasure of your correspondence by contacting us at [privacy@outbe.app](mailto:privacy@outbe.app).

#### **14. HOW CAN YOU CONTACT US ABOUT THIS POLICY?**

If you have questions or comments about this Policy, you may contact us by post at:

outbe App US Inc.  
5900 BALCONES DRIVE,  
SUITE 100 AUSTIN, TX  
78731 United States

For all privacy inquiries, you may contact [privacy@outbe.app](mailto:privacy@outbe.app).