PRIVACY POLICY

Date of last revision: 17 October 2025

INTRODUCTION & SCOPE

This Policy describes how **mirror US Inc. and mirror LT UAB** ("*Mirror*," "*we*," "*us*," or "*our*") process your personal information when you use our services.

Background information

Mirror operates as a Consumption Reflection Agent (CRA) in the outbe Network - a blockchain ecosystem where consumption creates value. We securely process your financial data (with your consent) to enable your participation in this new economic model, transforming everyday purchases into network contributions while protecting your privacy.

This Policy applies when you:

- Use a Wallet App that integrates CRA Services and links to this Policy;
- Authorize data access through the Wallet App, allowing Mirror to obtain access to your financial data from a Transaction Data Provider with your explicit consent;
- Receive CRA Outputs generated from your authorized data.
- Engage with us in other related ways.

Data Controller: Mirror acts as the data controller under applicable privacy laws. We determine how authorized financial data is processed to generate CRA Outputs. Wallet Apps operate independently and are governed by their own Terms of Use and Privacy Policies.

Jurisdiction: This Policy applies to the processing of personal information of individuals worldwide who use our Services. 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), UK GDPR, and other applicable local data protection regulations.

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 our Services. If you still have any questions or concerns, please contact us at privacy@mirror.tech.

IMPORTANT NOTICE: TECHNICAL ARCHITECTURE AND DATA RIGHTS

Zero-Storage Architecture: Mirror operates on a zero-storage architecture for personal data processing, meaning we process your data exclusively in temporary memory during active sessions. All personal information is automatically and irreversibly deleted immediately after generating and delivering CRA Outputs. This “Privacy by Design” approach ensures maximum data minimization and security by default.

Identity Limitations: We manage consent and data rights exclusively through blockchain wallet addresses as anonymous identifiers. Mirror cannot link wallet addresses to real-world identities, verify communication sources, or maintain user authentication systems.

Impact on Legal Rights: While you retain your fundamental rights under applicable data protection laws, the technical design of our zero-storage Services renders most data subject access, rectification, erasure, and portability rights inapplicable, as we do not retain any personal information upon which such rights could be exercised.

This limitation is recognized under GDPR Article 11(2), which specifies that where the controller cannot identify the data subject, the rights of access, rectification, erasure, and portability shall not apply. Similar provisions exist in the United States privacy laws, including California Civil Code § 1798.145(j)(2) .

By proceeding to use our Services after reviewing this notice, you provide informed consent to processing under these technical constraints and acknowledge that traditional data subject rights cannot be exercised due to technological impossibility, not unwillingness to comply.

Contact Email - Limited Capability: We maintain privacy@mirror.tech for general Policy questions and regulatory compliance inquiries. Due to our zero-storage architecture and our inability to verify identity, this email cannot assist with individual data access, deletion, or correction requests.

Your Data Control: You maintain full control through your Transaction Data Provider including the financial institution (who stores your financial data) and your Wallet App (which initiates processing sessions). For specific details about your control options, please see Section 9 below.

DEFINITIONS AND KEY TERMS

For purposes of this Policy:

"Services" means the Consumption Data aggregation, processing, and reporting services provided by Mirror, specifically the generation of CRA Outputs derived from financial data obtained from an authorized Transaction Data Provider.

"Consumption Data" means the specific details derived from your financial data that reflect your purchasing activities.

"CRA Outputs" means the two types of data we generate: Consumption Units and Consumption Reports.

"Consumption Units" means anonymized, cryptographically secured data products derived from your Consumption Data, containing no personally identifiable information, prepared for submission to the outbe Network.

"Consumption Reports" means personalized reports showing your Consumption Data, accessible only to you through the Wallet App to verify that the information is accurate.

"Transaction Data Provider" means the regulated entity that facilitates secure access to your payment account information. This term encompasses both (1) your financial institution (e.g., your bank) when it provides direct data access, and (2) authorized third-party providers (such as Account Information Service Providers or AISPs in Europe, data aggregators in the US, or similar entities in other jurisdictions), all operating in compliance with applicable regulations.

"Wallet App" means compatible third-party, non-custodial wallet applications through which you access our Services and connect your payment accounts. These applications operate independently under their own terms.

"*outbe Network*" means the decentralized blockchain ecosystem consisting of Layer 2 (privacy-preserving layer) and Layer 1 (blockchain), where your anonymized Consumption Units enable participation in network value creation mechanisms.

SUMMARY OF KEY POINTS

This summary provides key points from our Policy, but you can find out more details about any of these topics by clicking the link following each key point or by using our Table of Contents below to find the section you are looking for.

What personal information do we process?
Financial data obtained via Transaction Data Provider to generate cryptographically anonymized data products for blockchain integration. **[See Section 1]**

Do we process any sensitive personal information?
Yes, certain financial data we process may be considered “sensitive” under applicable laws. We process such data only with your consent or as otherwise permitted by law. **[See Section 1]**

Do we receive any information from third parties?
Yes, we receive data only from the Transaction Data Provider that you have authorized. We do not purchase data from data brokers. **[See Section 1]**

How do we process your information?
We process your information to provide our Services, generate privacy-preserving data products (CRA Outputs), and comply with applicable laws. We process information only when we have a valid legal reason to do so. **[See Section 2]**

In what situations and with which parties do we share personal information?
We do not share your personal information with third parties for their own use. We may share data only when compelled by law, though our technical architecture limits what we can provide. Our cloud infrastructure providers process encrypted data on our behalf but cannot technically access the underlying information. The Consumption Units we submit to the outbe Network are anonymized and contain no personal information. Your private Consumption Reports are not shared with any third parties. **[See Section 4]**

How long do we keep your information?
We do not keep your information. All data is processed in real-time and immediately deleted after generating CRA Outputs. [See Section 6]

How do we keep your information safe?
We maintain organizational and technical measures to protect your personal information, including encryption (both in transit and the rest) and restricted access controls. Our zero-storage architecture provides the primary security measure. **[See Section 7]**

What are your rights?
Depending on your location, applicable privacy law may grant certain rights regarding your personal information. Due to our zero-storage architecture, most rights are automatically fulfilled through immediate deletion. **[See Section 9]**

How do you exercise your rights?
Most data rights are automatically fulfilled by our zero-storage architecture. For general questions about our privacy practices, contact privacy@mirror.tech. **[See Section 9]**

Jurisdiction-Specific Rights:

- For EU, UK, and Swiss residents: See Section 9 for your specific privacy rights.
- For United States residents: See Section 11 for state-specific privacy rights.
- For all other jurisdictions: Your local data protection laws apply as described in Section 9.

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

TABLE OF CONTENTS

1. WHAT INFORMATION DO WE PROCESS?

In Short: *We process personal information that you explicitly authorize your financial institution to transmit to us, through a Transaction Data Provider, for the sole purpose of providing the Services*

Categories of Information Processed:

Category	Description	Source
Financial data	Transaction history (including merchant names, amounts, categories, merchant category codes (MCCs, or similar categorizations, and timestamps), account type, currency, and payment method details	Provided by Transaction Data Providers
Layer 2 Blockchain wallet address	Anonymized identifier required for technical operation. We have no means to link this address to your real-world identity.	Provided by your Wallet App
CRA Outputs	Consumption Units – anonymized data products for blockchain integration containing no personally identifiable information; Consumption Reports – personal reports accessible only to you through your Wallet App for verification. Reports enter a secure transit	Generated by us from your financial data

phase (not storage) where they remain encrypted and available for delivery to your Wallet App for up to 7 days, after which they are automatically deleted.

Sensitive Information: Where necessary, and only with your consent or as otherwise permitted by applicable law, we may process financial data obtained via a Transaction Data Provider (including transaction history, account type, currency, and payment method details), which may be considered sensitive under certain jurisdictions.

2. HOW DO WE PROCESS YOUR INFORMATION?

In Short: *We process your information to provide our Services and to comply with our legal obligations.*

We process your personal information to:

- **Connect to and process data from your payment accounts.** With your consent, we use an authorized Transaction Data Provider to securely access your financial data for CRA Outputs generation.
- **Deliver the Services.** We process your information to generate anonymized Consumption Units for blockchain integration and personal Consumption Reports for your verification.
- **Operate and improve our Services.** We analyze real-time system performance metrics that contain no personal information. These metrics (e.g., processing speed, error rates) are aggregated statistics that cannot be linked to any individual.
- **For Legal Purposes:** To comply with contractual and legal obligations under applicable law and for other legal purposes such as to establish and defend against claims.
- **Fulfill other purposes with your consent.** Any additional purposes will be communicated at the time of collection.

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 General Data Protection Regulation (EU GDPR) and the UK General Data Protection Regulation (UK GDPR) require us to explain the valid legal bases we rely on to process your personal information:

- **Consent:** Our primary legal basis for accessing your financial data is your explicit consent provided through your Transaction Data Provider. You can withdraw your consent at any time, as described in Section 9.
- **Contract performance:** Once you accept our Terms of Service, we process your data to fulfill our contractual obligations to provide the Services, including generating and delivering your CRA Outputs.
- **Legitimate Interests:** We have a legitimate interest in ensuring the technical operation and security of our service, specifically for system performance monitoring that involves no personal information. These interests are balanced against your fundamental rights and freedoms.
- **Legal Obligations:** We may be required to process data to comply with applicable laws and regulations, or valid requests from supervisory authorities. However, our ability to provide historical data is limited by our zero-storage architecture.

Legal Basis Framework

The table below specifies our legal basis for each processing activity:

Processing Activity	Personal information Categories	Legal Basis
Financial Data Access	Transaction history (including merchant names, amounts, categories, and timestamps), account type, and currency	Explicit Consent
CRA Outputs Generation	Financial data	Contract Performance
Layer 2 Network Submission	Cryptographic Units only, no personal information	Contract Performance
Service Improvement	System performance metrics only (no personal information)	Legitimate Interest
Responding to Lawful Requests	Financial data (real-time only) 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:

- **With service providers acting on our behalf.** We engage cloud infrastructure providers (for temporary processing environments). Due to our technical architecture and encryption methods, these providers cannot access any personal information we process - they only provide computing resources without visibility into the data itself. They must process the personal information in accordance with our contractual agreements and only as permitted by applicable data protections laws.
- **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. However, due to our zero-storage architecture, we can only provide information about our processing practices and policies, not historical user data.

- **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.

Anonymized Data Submission to outbe Network Infrastructure

As part of providing CRA Services, we submit Consumption Units to Layer 2 Network infrastructure. These submissions are fully anonymized with no personally identifiable information and enable your participation in the outbe Network ecosystem.

Important Limitation: Mirror's responsibility ends at Layer 2 Network submission of anonymized Consumption Units. Any subsequent submission to Layer 1 blockchain is initiated solely by you through your Wallet App and becomes permanently immutable.

What We Do NOT Share:

We will never share your personal information with marketing companies, data brokers, advertisers, or provide Consumption Reports to any third parties.

5. IS YOUR INFORMATION TRANSFERRED INTERNATIONALLY?

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

To support our global Services, we maintain secure data centers in the United States and the European Union. The location where your information is processed depends on your country of residence:

- **For users in the United States**: Your personal information is processed on our US-based servers.
- **For users in the European Economic Area (EEA) and the UK**: We prioritize processing your personal information on our EU-based servers. A transfer to our US-based servers may only occur if protected by the safeguards described below.
- For users in all other countries: By using our Services, you acknowledge that your personal information may be transferred to and processed in either the United States or the European Union.

Please be aware that the countries where we operate may not provide the same level of data protection as your home jurisdiction. However, we implement comprehensive safeguards to protect your personal information in accordance with this Policy and applicable law.

International Transfer Safeguards

European Commission's Standard Contractual Clauses (SCCs)

We use the European Commission's Standard Contractual Clauses for transfers of personal information from the EEA and UK, if applicable, and implement equivalent contractual

safeguards for transfers from other jurisdictions where required by local law. These clauses require all recipients to protect all personal information in accordance with applicable data protection laws and regulations. Our Standard Contractual Clauses can be provided upon request. We have implemented similar safeguards with our third-party service providers and partners, and further details can be provided upon request. We conduct Transfer Impact Assessments (TIAs) for all international data transfers, evaluating local surveillance laws and implementing additional safeguards where needed.

For UK residents: Following Brexit, the UK has adopted UK GDPR which mirrors EU GDPR. We rely on the UK's adequacy decision for EU-UK transfers and implement UK-specific Standard Contractual Clauses where required.

Additional Jurisdictional Safeguards

For jurisdictions without formal adequacy decisions or framework agreements, we implement:

- Contractual protections based on GDPR Article 46 safeguards.
- Transfer Impact Assessments (TIAs) evaluating local surveillance laws and privacy risks.
- Enhanced encryption with jurisdiction-specific key management protocols.
- Data localization where legally required.
- Emergency procedures for immediate data isolation if legal changes pose unacceptable privacy risks.

Anonymized Data Processing: Anonymized Consumption Units submitted to Layer 2 Network infrastructure may be processed across multiple jurisdictions where outbe Network nodes operate. These submissions contain only Consumption Units with no personally identifiable information.

6. HOW LONG DO WE KEEP YOUR INFORMATION?

In Short: *We do not keep your information. All data is processed in real-time and immediately deleted after generating CRA Outputs.*

We apply a strict zero-retention policy:

Data Type	Retention Period	Purpose
Financial data	Zero - processed in memory only	Generate CRA Outputs

Data Type	Retention Period	Purpose
Consumption Units	Zero - immediately submitted to Layer 2	outbe Network submission
Consumption Reports	Encrypted in transit phase: Maximum 7 days OR until Wallet App confirms receipt (whichever occurs first)	User verification

Transit Phase:

Consumption Reports remain encrypted in transit phase pending delivery to your Wallet App. This ensures:

- Reports remain encrypted and accessible only through your Wallet App.
- Automatic deletion upon successful delivery confirmation.
- Maximum 7-day delivery window before automatic purge.
- Reliable delivery despite network latency or connection issues.

Key Retention Principles:

- **Financial data** obtained via Transaction Data Provider are processed in memory only to generate the CRA Outputs, then immediately deleted.
- **Consumption Units** are created during the processing session and submitted to Layer 2 Network immediately, with no copies retained by Mirror.
- **Consumption Reports** are generated and made available to you only. These reports remain encrypted in transit phase only until successfully delivered to you (maximum 7 days).

Important note regarding blockchain immutability: While Mirror does not retain your data beyond the processing session, data you choose to submit to Layer 1 blockchain through your Wallet App will become permanently immutable records that cannot be deleted, modified, or controlled by Mirror.

7. HOW DO WE KEEP YOUR INFORMATION SAFE?

In Short: *Our primary security measure is our zero-storage architecture, supplemented by appropriate technical and organizational measures.*

We have implemented appropriate technical and organizational security measures. Our primary security measure is our zero-storage architecture, which ensures your data is immediately and irreversibly deleted after processing. These measures also include:

Data Protection Measures:

- Encryption of all your information during transit and at the rest during processing.
- Anonymization using hashing algorithms and aggregation before any outbe Network submission.
- Segregated processing environments ensuring financial data never co-mingles with blockchain-ready data.

System Security Measures:

- Multi-factor authentication for all administrative access.
- Regular security audits and penetration testing.
- Incident response procedures including notification protocols for data breaches as required by law.
- Access control in information security.
- Authentication requirements in authentication and authorization.

Organizational Measures:

- Strict access controls ensuring that only authorized personnel with a legitimate business need can access systems.
- Regular privacy and security training for all employees.
- Data Protection Impact Assessments (DPIAs) conducted for new processing activities.
- Business continuity and disaster recovery plans.

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

However, no electronic transmission over the Internet or information storage technology can be guaranteed to be 100% secure. Transmission of personal information to and from our Services is at your own risk.

8. DO WE PROCESS INFORMATION FROM MINORS?

In Short: *We do not knowingly process data from or market to children under 13 years of age or individuals under 18 years of age.*

We do not knowingly process financial data from children under 13 years of age (in compliance with COPPA) or from individuals under 18 years of age, nor do we knowingly sell such personal information. By using the Services, you represent that you are at least 18 years old.

Technical Limitations: Due to our zero-storage architecture and the nature of our data processing, we have no direct means to verify the age of individuals whose financial data we process. We cannot identify users beyond their blockchain wallet addresses, which provide no age-related information.

Parents and guardians are responsible for monitoring and controlling access to financial accounts and wallet applications on devices accessible to minors. If you believe a child under 13 has gained unauthorized access to our Services through your accounts, please revoke the relevant authorizations through your Transaction Data Provider or Wallet App immediately.

9. WHAT ARE YOUR PRIVACY RIGHTS?

In Short: *Due to our zero-storage architecture, most data rights are automatically fulfilled.*

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

(i) to request access and obtain a copy of your personal information,
(ii) to request rectification or erasure;
(iii) to restrict the processing of your personal information;
(iv) if applicable, to data portability;
(v) not to be subject to automated decision-making
(vi) to object to the processing of your personal information.

Technical Limitations on Rights Implementation

Due to our zero-storage architecture, certain rights are inherently satisfied while others cannot be technically fulfilled:

Right	Status	Explanation
Right to erasure	Automatically fulfilled	All data deleted after processing
Right to restriction	Automatically fulfilled	Processing occurs only during your session
Right to object	Available	You can prevent processing by not initiating sessions
Right to withdraw consent	Available	Withdraw through Transaction Data Provider or Wallet App
Right to portability	Technically Infeasible	No data stored to transfer
Right to access	Technically Infeasible	Per GDPR Article 11(2) - we cannot identify you or retrieve past data
Right to rectification	Technically Infeasible	No data retained to correct
Right not to be subject to automated decision-making	Fulfilled	We do not engage in automated decision-making with legal effects

How to Exercise Your Rights

For general privacy inquiries only, contact privacy@mirror.tech. Please note that we cannot verify your identity from your email address or fulfill individual data requests as we maintain no user records or stored data.

We aim to respond to all privacy rights requests as quickly as possible. If we are unable to respond within 10 working days, we will inform you in writing of the timeline for our response. If we cannot fulfill your request, we will explain the reasons (unless prohibited by applicable laws).

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 or manage data sharing permissions directly with your Transaction Data Provider, including your financial institution.

Complaints to Data Protection Authorities

While we encourage you to contact us first at privacy@mirror.tech 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, even though individual data requests cannot be fulfilled due to our zero-storage architecture.

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.
- **UK residents**: Contact the Information Commissioner's Office (ICO).
- **Swiss residents**: Contact the Federal Data Protection and Information Commissioner.

Limitations on your rights

Your rights may be limited where:

- Fulfilling your request would reveal personal information about another person.
- We have compelling legitimate grounds that override your interests.
- Technical impossibility exists (e.g., for blockchain data once submitted to Layer 1).
- Legal obligations require us to maintain certain processing.

10. CONTROLS FOR DO-NOT-TRACK FEATURES

Most web browsers and some mobile operating systems and mobile applications include a Do-Not-Track ("DNT") feature or setting you can activate to signal your privacy preference not to have data about your online browsing activities monitored and collected. Since Mirror does not engage in tracking or collect browsing data, DNT 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. If a standard for online tracking is adopted that we must follow in the future, we will inform you about that practice in a revised version of this Policy.

California law requires us to let you know how we respond to web browser DNT signals. Because there currently is not an industry or legal standard for recognizing or honoring DNT signals, we do not respond to them at this time.

11. DO UNITED STATES RESIDENTS HAVE SPECIFIC PRIVACY RIGHTS?

In Short: *I: 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. However, most are automatically fulfilled through our zero-storage design.*

Categories of Personal Information We Process

Category	Illustrative Examples	Processed	Data We Process
A. Identifiers	Contact details, such as real name, alias, postal address, telephone or mobile contact number, unique personal identifier, online identifier, Internet Protocol address, email address, and account name	YES	Layer 2 Blockchain wallet address
B. Personal information as defined in the California Customer Records statute	Name, contact information, education, employment, employment history, and financial information	YES	Financial information
D. Commercial information	Transaction information, financial details, and payment information	YES	Transaction information (including merchant names, locations, amounts, and merchant category codes)
L. Sensitive personal Information	Payment account identifiers, account access details, and transaction history	YES	Payment account data (including transaction history from your linked accounts)

We only process sensitive personal information, as defined by applicable privacy laws, for the purposes allowed by law or with your consent. Sensitive personal information may be used, or disclosed to a service provider or contractor, for additional, specified purposes. You may have the right to limit the use or disclosure of your sensitive personal information. We do not process sensitive personal information for the purpose of inferring characteristics about you.

We may also process other personal information when you send inquiries to our general privacy email address.

Retention

All categories: Zero - processed in memory only. The resulting anonymized Consumption Units are submitted to the network, and you have sole control over your Consumption Reports.

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.

Notice of Sale/Sharing Practices: We do not and will not sell or share your personal information as defined under California law.

Global Privacy Control: We recognize automated opt-out preference signals. However, our zero-storage architecture means there is no ongoing processing from which to opt out.

Your Rights

You have rights under certain United States data protection laws, including:

- **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 profiling.

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)

Important Note: Due to our zero-storage architecture, most rights are automatically fulfilled. We cannot verify identity or connect requests to any data.

How to Exercise Your Rights

For general privacy inquiries, contact privacy@mirror.tech.

Appeals

Under certain United States data protection laws, you have the right to appeal our decision if we decline to take action on your request. Because Mirror cannot identify individual users, an appeal can only challenge our general privacy policies. You may submit an appeal to

privacy@mirror.tech. We will provide a written response within 10 working days 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@mirror.tech.

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 "Revised" date at the top of this Policy. If we make material changes, we may notify you either by prominently posting a notice through 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@mirror.tech, we process the personal information you provide to us. This processing is separate from the data processing that occurs when you use our core Services and is governed by different rules as described below:

- **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.
- **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.
- **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.
- **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.

- **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@mirror.tech. Please note that exercising these rights applies only to the data related to your direct communications with us and not to any data processed through our zero-storage core Services, for which such rights remain technologically infeasible to fulfill.

14. HOW CAN YOU CONTACT US ABOUT THIS POLICY?

If you have questions or comments about this policy, email us at privacy@mirror.tech or contact us by post at:

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

mirror LT UAB
Domicelės Tarabildienės g. 3, LT-25128
Vilnius, Lithuania
Email: eu-privacy@mirror.tech