

Divindi Privacy Policy

Last updated: October 15, 2026

This Privacy Policy explains how **Divindi LLC** ("**Divindi**", "**we**", "**us**", "**our**") collects, uses, shares, and protects personal information when you use the Divindi mobile application (including the Divindi consumer app and the Divindi Business app), our websites, and related services (the "**Services**"). It also explains the choices and rights you have.

Divindi is the **controller** (or "business") responsible for the personal information described here, except where this Policy says that a partner acts as an independent controller.

Contact: Divindi LLC, 2121 Market Street, Galveston, Texas 77550, USA, hello@divindi.tech.

1. Summary

- To open and protect your account, and to meet anti-fraud, anti-money-laundering, and sanctions obligations, we verify your identity using **Persona**. Persona collects an image of your government ID and a selfie, and uses **facial biometrics** to confirm that you are the person on the ID. **Divindi's own systems do not receive or store your selfie, face images, or any biometric identifier or template.** See Section 5.
- Your sensitive identity details (ID document images, ID number, date of birth, tax ID, source of funds, and similar information) are **passed to our banking partner Bridge for its own checks, and are not stored in Divindi's databases.**
- Personal information we do store is **encrypted at rest**, using encryption keys held in hardware security modules.
- We **do not sell** your personal information, we **do not share it for cross-context behavioral advertising**, and the app contains **no advertising or cross-app tracking SDKs.**
- You can **delete your account in the app** at any time, and you can contact us to exercise your other privacy rights.
- Payments are recorded on **public blockchains**. Blockchain records are public and permanent, and nobody, including Divindi, can delete them.

2. Information we collect

2.1 Information you give us

Category	Examples	When
Sign-in and contact details	Email address and/or mobile phone number, and the one-time codes used to verify them	When you create an account or sign in
Profile details	Legal first and last name, country of residence, residential address, optional @username	When you set up your account

Category	Examples	When
Identity verification information	Images of your government-issued ID (front and back), the information printed on it (such as name, date of birth, document number, nationality, place of birth, issuing country, and expiry), and a selfie photo or short video of your face	During identity verification, collected by Persona on our behalf (Section 5)
Due-diligence information for bank services	Purpose of account, employment status, occupation, source of funds, expected activity, whether you act on behalf of someone else, tax identification number (for example SSN or ITIN), and anything else Bridge requires	When you enable bank deposits and withdrawals; sent to Bridge and not stored by Divindi
Recipients you save	Names, @usernames, blockchain addresses, and bank payout details you save for people you pay	When you add a recipient
Payment information	Transaction amounts, assets, recipients, merchants, references, and notes	When you send, pay, exchange, deposit, withdraw, or schedule a payment
Business information (Divindi Business only)	Business name, payment and order details, and, if you connect Square, your Square merchant and location information	When you use the Business app
Communications	Messages you send to support, and feedback	When you contact us

2.2 Information collected automatically

Category	Examples	Purpose
Account and device credentials	Passkey public keys and credential identifiers, a device name you can see in "Your devices", session tokens	Signing you in, approving transactions, managing your devices. Your passkey private keys stay on your device and in your platform's passkey manager (e.g., iCloud Keychain or Google Password Manager); we never receive them.
Blockchain account data	Your blockchain account name and addresses, balances, and on-chain transaction records	Showing your balance and activity, executing transactions
Push notification token	An Expo push token for your device	Sending account, payment, and security notifications
Diagnostics	Crash reports, error details, app version, device type, and operating system, tagged with an internal account identifier	Finding and fixing errors (via Sentry)
Product analytics	Which screens are used (by screen type, not by content), and the outcome of steps in flows such as a withdrawal, scheduled payment, or pocket operation, linked to a pseudonymous customer identifier	Understanding and improving the app (via PostHog). Analytics events are designed to exclude names, contact details, addresses, and amounts.

Category	Examples	Purpose
Security and audit logs	Records of sign-ins, device changes, recovery events, and administrative actions, with IP-derived and request metadata	Security, fraud prevention, and legal record-keeping

2.3 Device permissions

The app asks for your permission before using these device features, and you can turn them off in your device settings:

- **Camera.** Used to scan payment QR codes and device-pairing codes, and inside Persona's verification flow to photograph your ID and take your selfie. Divindi does not save camera images.
- **NFC.** Used to read payment requests from merchant terminals.
- **Notifications.** Used for payment, account, and security alerts.
- **Biometric unlock (Face ID, Touch ID, fingerprint).** Used by your device's operating system to unlock your passkeys and the optional App Lock. **This biometric check happens entirely on your device; Divindi never receives your fingerprint or face data from it.**
- **Clipboard.** The app reads your clipboard only when you tap a "paste" action, for example to paste a payment link.

We do not collect your precise or approximate location from your device's location services, your phone's address book, or microphone audio, and we do not track you across other companies' apps or websites.

2.4 Information from third parties

- **Persona:** the result of your identity verification (approved or declined, and which checks passed), Persona reference identifiers, and the verified identity attributes and document images described in Section 5, which we pass to Bridge.
- **Bridge:** your Bridge customer and account identifiers, the status of Bridge's verification and of your bank transfers, and whether you accepted Bridge's terms.
- **Stytch:** confirmation that you control the email address or phone number you sign in with.
- **Stripe:** the status of card purchases you make through Stripe.
- **Public blockchains:** transaction and balance data related to your addresses.
- **Sanctions and risk screening sources:** results of screening names, addresses, and blockchain addresses against sanctions and risk lists.

3. How we use personal information

Purpose	Information used	Legal basis (EEA/UK)
Opening and running your account; providing payments, exchange, bank transfers, pockets, scheduled payments, statements, and support	Sign-in, profile, payment, recipient, device, and blockchain data	Performance of our contract with you

Purpose	Information used	Legal basis (EEA/UK)
Verifying your identity at sign-up and, for account recovery , confirming that the person recovering is the enrolled account holder	Identity verification information, including biometric information processed by Persona	Legal obligation; legitimate interest in preventing fraud and account takeover; your explicit consent for biometric processing
Meeting anti-money-laundering, counter-terrorist-financing, sanctions, tax, and record-keeping obligations, including screening transactions and blocking prohibited ones	Identity, profile, payment, and blockchain data	Legal obligation; legitimate interests
Detecting, preventing, and investigating fraud, abuse, and security incidents	Device, log, payment, and verification data	Legitimate interests; legal obligation
Sending service, security, and transaction notifications	Contact details and push tokens	Performance of contract; legitimate interests
Diagnosing errors and improving the Services	Diagnostics and product analytics	Legitimate interests (you can object, see Section 9)
Complying with law, responding to lawful requests, and enforcing our Terms	Any relevant information	Legal obligation; legitimate interests

We do not use your personal information for automated decisions that produce legal or similarly significant effects without human involvement, except automated identity verification and sanctions screening required to open an account and keep it compliant. If your verification is declined, you can contact us to ask for a human review.

We do not use your personal information, including identity documents or biometric information, to train artificial-intelligence models.

4. How we share personal information

We share personal information only as described below. **We do not sell personal information, and we do not "share" it for cross-context behavioral advertising** (as those terms are defined in the California Consumer Privacy Act).

4.1 Service providers (processors)

These companies process personal information on our behalf, under contracts that limit how they can use it:

Provider	What it does for us	Information involved
Persona Identities, Inc.	Identity verification, document authentication, liveness detection, and face matching	Identity verification information, including biometric information
Stytch, Inc.	Sign-in and verification of email addresses and phone numbers	Email address, phone number, sign-in events

Provider	What it does for us	Information involved
Google Cloud	Hardware security modules for encryption and signing keys; security log storage	Encrypted key material; security logs
Railway	Hosting for our servers and databases	All information we store
Sentry	Error and crash reporting	Diagnostics, internal account identifier
PostHog	Product analytics	Pseudonymous identifier and usage events
Expo (with Apple Push Notification service and Firebase Cloud Messaging)	Delivering push notifications	Push token, notification content

4.2 Partners that provide services to you

These partners receive information so they can provide their own services to you, and they act as independent controllers under their own privacy policies:

- **Bridge** (bridge.xyz; Bridge Building Inc. for U.S. customers, Bridge Building S.A. for EEA customers, and Bridge Building Limited elsewhere) and its banking partners: bank account details, deposits, withdrawals, and their own customer due diligence. We send Bridge your name, verified email address and phone number, residential address, date of birth, nationality, place of birth, government ID details and (for non-U.S. residents) ID images, tax identification number, and due-diligence answers. Bridge may ask you for more information, such as a proof-of-address document or its own selfie check, through its own flow.
- **Stripe, Inc.**, if you buy stablecoins by card.
- **Square, Inc.**, if you connect a Square account in the Divindi Business app.
- **Your bank or a partner's app**, if you use a partner-branded version of Divindi.

4.3 Blockchains and other participants in a transaction

When you make a transaction, the information needed to complete it is shared with the recipient or merchant, and with blockchain networks, the NEAR Intents protocol, and independent market makers ("solvers") that fill exchanges. **Transactions, amounts, and blockchain account names and addresses, including your @username, are permanently and publicly visible on blockchains.** We do not put your legal name, contact details, or identity documents on-chain.

4.4 Other disclosures

We may disclose personal information: to comply with law, regulation, legal process, or a government or regulatory request; to protect the rights, property, or safety of you, our users, Divindi, or others, including to prevent fraud; to professional advisers under a duty of confidentiality; and, with appropriate safeguards, to a buyer or successor in a merger, acquisition, financing, or sale of assets, in which case we will tell you about any change in who controls your information.

5. Biometric information and identity verification

This section is our notice and policy on biometric information. It applies in addition to the rest of this Policy, including for residents of Illinois, Texas, Washington, Colorado, and other places with biometric privacy laws.

5.1 What is collected and by whom. When you verify your identity, our service provider **Persona Identities, Inc.** collects images of your government-issued ID and a selfie photo or short video of your face. Persona uses them to check that the ID is genuine, that a live person is present (liveness detection), and that your face matches the photo on your ID. To do this, Persona may create **face geometry or other biometric identifiers or information ("Biometric Information")** from those images.

5.2 Account recovery. If you lose every device on your account and ask to recover it, Persona collects a new selfie and **compares it with the selfie from your original verification** to confirm that the person recovering is the enrolled account holder. This protects your account from takeover. Your enrollment verification is kept for this purpose while your account is open.

5.3 What Divindi receives. Divindi's systems do not receive or store your Biometric Information, selfies, or face images. These remain with Persona. A small number of authorized Divindi compliance personnel may view a verification, including its images, in Persona's secure, access-controlled dashboard, only when needed to review a declined or flagged verification or to investigate suspected fraud. We receive only the outcome of each verification (for example, whether the ID check, the selfie check, and the face comparison passed) and Persona's reference identifiers for your verification. We store those references encrypted. We also receive from Persona the identity details printed on your ID and, for non-U.S. residents, the ID document images. We pass them directly to Bridge for its own customer due diligence, without writing them to our databases, file storage, or logs.

5.4 Purpose and consent. Biometric Information is collected and used only to verify your identity, prevent fraud and account takeover, and meet legal obligations. **Before any Biometric Information is collected, you will be asked in the verification flow for your written consent** to the collection, use, and storage of your Biometric Information by Persona on Divindi's behalf, for these purposes and for the retention period below. If you do not consent, we cannot verify your identity, and we will not be able to open your account or complete a recovery.

5.5 No sale or profit. Neither Divindi nor Persona will sell, lease, trade, or otherwise profit from your Biometric Information. It will not be disclosed except to Persona and Persona's own sub-processors to provide the verification, or where required by law, a valid warrant, or a subpoena.

5.6 Retention and destruction. Biometric Information is kept only as long as needed for the purposes above. Biometric Information from a sign-up verification is kept while your account is open, so it can be used in account recovery. It is **permanently destroyed no later than one year after the purpose for collecting it ends** (for example, one year after your account is closed or deleted, or after a verification that did not result in an account), **and in any case no later than three years after your last interaction with Divindi**, unless a longer period is required by law or a valid legal process. Persona applies this schedule on our instructions.

5.7 Security. Biometric Information is protected with at least the same care we use for our other most sensitive information, including encryption in transit and at rest and strict access controls at Persona.

5.8 Persona's policy. Persona's handling of personal information is also described in its privacy policy at withpersona.com/legal/privacy-policy. To exercise rights over verification data, contact Divindi first (Section 9). Persona processes this data as our service provider.

6. How long we keep personal information

We keep personal information only as long as needed for the purposes in this Policy, including legal, regulatory, tax, and accounting requirements. Our main retention periods are:

Information	Retention
Sign-in sessions and one-time sign-in challenges	Deleted soon after they expire (session lineage at most 30 days after expiry)
Passkey records, device list, recovery data, recipients, push tokens, preferences	While your account is open; deleted when you delete them or delete your account
Transaction, activity, and ledger records	7 years from the transaction (financial record-keeping)
Payment requests	2 years after payment or expiry
References linking you to Bridge, and records of your acceptance of Bridge's terms	Life of the account plus 5 years (anti-money-laundering record-keeping)
Security and audit logs	At least 1 year, up to 7 years
Diagnostic and operational logs	About 90 days
ID document images, ID number, date of birth, tax ID, due-diligence answers	Not stored by Divindi ; passed to Bridge in transit only
Biometric Information	Not held by Divindi; held by Persona as described in Section 5.6
Persona and Bridge records	Held by those companies under their own legal obligations and our instructions

When retention ends, we delete the information or make it permanently unreadable by destroying its encryption key ("crypto-shredding"). Backups expire on a rolling schedule. Information subject to a legal hold is kept until the hold ends.

7. How we protect personal information

We protect personal information with administrative, technical, and physical safeguards, including:

- encryption in transit (TLS) and **encryption at rest of the personal information we store**, using per-record AES-256-GCM keys that are themselves protected by non-exportable keys in Google Cloud hardware security modules;
- **data minimization**: the most sensitive identity data is never stored in our systems;
- passkey-based sign-in and transaction approval, so there is no password or seed phrase to steal;
- smart-contract controls that delay account recovery and let any of your devices cancel it;

- least-privilege access, logging of privileged actions, secret scanning, and an incident response process.

No system is perfectly secure. If a security breach affects your personal information, we will notify you and the authorities as required by law.

8. International transfers

Divindi is based in the United States, and our providers process information in the United States, the European Union, and other countries. Where we transfer personal information from the EEA, the United Kingdom, or Switzerland to a country without an adequacy decision, we use appropriate safeguards, such as the European Commission's Standard Contractual Clauses (and the UK Addendum) or a provider's certification under the EU-U.S. Data Privacy Framework.

9. Your rights and choices

9.1 Rights for everyone. Wherever you live, you can ask us to:

- **access** the personal information we hold about you and receive a copy in a portable format;
- **correct** inaccurate information;
- **delete** your information. You can delete your account yourself in **Settings > Delete account**. This permanently erases your sign-in, passkeys, saved recipients, scheduled payments, notification tokens, referral links, and recovery data, and destroys the encryption key for your encrypted records. We keep only the records we are legally required to keep (Section 6). On request, we will ask Persona and Bridge to delete the information they hold for us, subject to their own legal obligations;
- **object to or restrict** certain processing, including product analytics;
- **withdraw consent** where we rely on it, including consent to biometric processing. Withdrawing consent does not affect processing that already happened, and may mean we cannot provide services that require identity verification.

To make a request, email **hello@divindi.tech** from the email address on your account, or contact us through the app. To protect you, we verify requests before acting on them, and we may ask for more information. You may use an authorized agent where the law allows; we may ask the agent for proof of authority. We respond within the time the law requires (generally within 30 days in the EEA and UK, and 45 days in U.S. states, extendable where permitted). **We will not discriminate against you for exercising your rights.** If we deny your request, you may appeal by replying to our decision, and we will respond to your appeal as the law requires.

9.2 EEA, UK, and Swiss residents. You have the rights above under the GDPR and UK GDPR, including the right to data portability and to object to processing based on legitimate interests. You may lodge a complaint with your local data protection authority.

9.3 California residents. In the last 12 months we have collected these categories of personal information under the CCPA: identifiers; customer records information (Cal. Civ. Code §1798.80(e)); characteristics of protected classifications (age and nationality); commercial information (transaction history); biometric information (collected and processed by Persona as our service provider, not received by Divindi); internet or other electronic network activity information; sensory information (ID and selfie images); professional or

employment-related information (employment status and occupation, for bank due diligence); and inferences limited to fraud and risk signals. The sources, purposes, and recipients are described in Sections 2 to 4, and retention in Section 6. **Sensitive personal information** (government ID numbers, SSN, account sign-in credentials, biometric information, and precise financial data) is used only for purposes permitted by CCPA regulations §7027(m), such as providing the Services, security, and legal compliance. We do not use or disclose it to infer characteristics about you. **We do not sell or share personal information, and have no actual knowledge of selling or sharing the information of anyone under 16.** California's "Shine the Light" law does not apply because we do not disclose personal information to third parties for their direct marketing purposes.

9.4 Other U.S. states. If you live in Colorado, Connecticut, Delaware, Iowa, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Texas, Utah, Virginia, or another state with a consumer privacy law, you have the rights to access, correct, delete, and obtain a copy of your information, to opt out of sale, targeted advertising, and profiling (we do none of these), and to appeal our decisions. Note that some financial information is governed by the federal Gramm-Leach-Bliley Act rather than these state laws.

9.5 Global Privacy Control and Do Not Track. We do not sell or share personal information or engage in targeted advertising, so there is nothing for these signals to opt you out of. Where the law requires it, we treat a Global Privacy Control signal as a valid opt-out request.

9.6 Notifications. You can turn push notifications off in your device settings. We will still send messages required for security, legal, or transactional reasons.

10. Children

The Services are not for anyone under 18. We do not knowingly collect personal information from children. If you believe a child has given us personal information, contact us and we will delete it.

11. Cookies and our websites

The Divindi app does not use advertising cookies. Some steps open pages run by our partners (such as Persona's verification flow and Bridge's terms and bank-account pages) inside the app. Those pages may use cookies or similar technologies that are strictly necessary for them to work, under those partners' policies. Our websites use only cookies and local storage needed to operate them. If we ever add analytics or advertising cookies to our websites, we will update this Policy and ask for consent where required.

12. Third-party links and services

The Services link to third-party services, such as Bridge, Stripe, Square, Persona, app stores, and blockchain explorers, that have their own privacy practices. This Policy does not cover them, and we encourage you to read their policies.

13. Changes to this Policy

We may update this Policy. If we make material changes, we will notify you in the app or by email before the changes take effect, and where the law requires it, we will ask for your consent. The "Last updated" date shows when this Policy last changed.

14. Contact us

Divindi LLC Attn: Privacy 2121 Market Street, Galveston, Texas 77550, USA Email: **hello@divindi.tech**

Divindi LLC · 2121 Market Street, Galveston, Texas 77550, USA · Divindi Privacy Policy · Effective October 15, 2026