

GotSOL Privacy Policy

Effective Date: September 20, 2025

Entity: GotSOL, LLC (“GotSOL”, “Company”, “we”, “us”, or “our”)

Contact (Privacy Requests): gotsol-biz@protonmail.com (subject: “Privacy Request”)

Postal Address: []

1. Introduction & Scope

This Privacy Policy explains how we collect, use, disclose, and safeguard Personal Information when you use our **non-custodial Solana-based merchant payment platform and related tools** (the “Service”). By using the Service, you agree to this Policy and our Terms of Service.

Roles (Controller vs. Processor/Service Provider)

- **Controller.** GotSOL is a **controller** for account/admin data, communications, security/risk, product analytics (with consent where required), and marketing.
- **Processor/Service Provider.** For certain merchant features (e.g., merchant-configured fields about their end-customers), we act as a **processor/service provider** under a **Data Processing Addendum (DPA)** and the merchant’s documented instructions. Under CPRA we act as a **service provider/contractor** and will not **sell** or **share** that data, will not use it beyond the business purpose, and will assist the merchant in responding to consumer requests.

Blockchain Limitation (Important): Transactions on Solana are public, permanent, and **cannot** be deleted, modified, or made private by GotSOL.

2. Information We Collect

2.1 You Provide Directly

- **Account & Business Info:** email, username, merchant name, role/permissions, owner/administrator details.
- **Communications:** support tickets, chat, email correspondence, feedback.

- **Payments/Transactions:** public wallet addresses (keys), amounts, token mints, timestamps, transaction signatures.
- **Customer Data (merchant-provided):** optional merchant-configured fields about customers and payment preferences.

2.2 Collected Automatically

- **Usage & Device:** feature usage, event logs, crash logs, approximate location from IP, browser/OS/device, referrers.
- **Cookies/Local Storage/PWA:** session tokens, preferences, app state, offline caches (IndexedDB/Service Worker).
- **Blockchain:** public on-chain records (hashes, addresses, amounts, timestamps) indexed for functionality, fraud detection, and reconciliation.

2.3 From Third Parties

- **Privy** (wallet/auth), **Supabase** (database/session), **Jupiter/HeroSwap** (swap routing metadata), hosting/analytics/service tools.
- **Public Sources:** public blockchain and generally available sources.

3. How We Use Personal Information

- **Provide & Operate:** authenticate, maintain sessions, enable merchant payment processing, integrate with third-party services you choose.
- **Security & Compliance:** detect/prevent fraud/abuse, protect accounts, comply with legal obligations (including sanctions screening if required), enforce Terms.
- **Communications:** respond to inquiries, send service notices and security updates; where permitted, send product news (you may opt out).
- **Improvement & Analytics:** understand performance, improve features, and conduct research (consent where required).

- **Legal Defense/Claims:** establish, exercise, or defend legal claims.

4. Legal Bases (if GDPR/UK GDPR applies)

- **Contract** (Art. 6(1)(b)); **Legitimate Interests** (Art. 6(1)(f), e.g., security/fraud and essential analytics balanced against rights); **Consent** (Art. 6(1)(a) for non-essential cookies/marketing); **Legal Obligation** (Art. 6(1)(c)).

5. Cookies, Local Storage & Tracking

- **Essential** cookies/local storage are required for login, security, and PWA/offline features.
- **Non-essential** analytics/ads (if used) require consent where applicable; you can manage preferences via our banner and browser settings.
- **Global Privacy Control (GPC):** where required (e.g., CA), we honor GPC signals as an opt-out of “sale”/“sharing.”
- **Do Not Track (DNT):** we do **not** respond to DNT signals.

6. Disclosures of Personal Information

We **do not** sell Personal Information for money. We disclose Personal Information to:

- **Service Providers/Processors:** Privy, Supabase, hosting, analytics, support, and other vendors under contracts restricting their use (including CPRA service provider/contractor terms).
- **Integration Partners:** Jupiter/HeroSwap and similar partners to enable functionality you request.
- **Compliance & Safety:** regulators, law enforcement, or parties to legal processes when required or to protect rights, property, and safety.
- **Corporate Events:** merger, acquisition, financing, or asset transfer under consistent safeguards.

CPRA “Sharing.” Some analytics/ads (if used) may be deemed “sharing” for cross-context behavioral advertising; you may **opt out** via our banner or GPC.

7. Blockchain Transparency (Important)

Solana transactions are **public and immutable**. On-chain data cannot be deleted or altered by GotSOL. Public addresses may be linkable to behavioral patterns or your identity if you disclose it elsewhere. Consider the **physical and competitive risks** of public financial records before using the Service.

8. Security

We implement **commercially reasonable** administrative, technical, and organizational measures—such as TLS in transit, access controls, monitoring, and backups—designed to protect Personal Information. **No method is 100% secure**, particularly for public blockchain activity, and we cannot guarantee absolute security.

9. Retention

We retain Personal Information **only as long as necessary** for the purposes stated or as required by law:

- **Account/Support:** account lifetime + up to **3 years** after closure.
- **Security/Logs:** typically **12–24 months**, longer if needed for investigations/legal obligations.
- **KYC/Compliance (if collected):** **5–7 years** where required.
- **Marketing:** until you opt out or withdraw consent.
Blockchain data is public and outside our control; it is not subject to deletion or correction by GotSOL.

We may retain **aggregated/de-identified** information (that cannot reasonably be linked to you) for analytics and improvement.

10. Your Rights & Choices

Depending on your jurisdiction, you may have rights to **access/know, correct, delete, port, opt out** of “sale”/“sharing” and targeted advertising, **limit** the use of **sensitive** Personal Information (if collected), **object** or **restrict** processing, **withdraw consent** (for optional processing), and **appeal** a denied request.

How to Exercise: email gotsol-biz@protonmail.com (subject: “Privacy Request”). Include your name, jurisdiction, and the email/account used.

Verification: we may request reasonable verification (e.g., email confirmation and limited additional info).

Authorized Agents (CA): permitted with verifiable authorization.

Timelines: we respond within applicable statutory periods (e.g., **45 days** in CA, extendable as permitted).

Non-Discrimination: we will not discriminate against you for exercising your rights.

Blockchain Limitation: deletion/correction **does not apply** to on-chain records.

11. Privacy For Minors

The Service is **not intended for individuals under 18**. We **do not knowingly collect** Personal Information from children under 13 (COPPA). If you believe a child provided data, contact us to request deletion where feasible (on-chain records cannot be removed).

12. International Data Transfers

We may process data in the United States and other countries. For EEA/UK transfers we rely on **Standard Contractual Clauses** (and UK Addendum, as applicable) and apply additional safeguards as appropriate.

13. Third-Party Services & Subprocessors

We integrate with **Privy** (wallet/auth), **Supabase** (database/session), **Jupiter/HeroSwap** (swap routing), and other SaaS providers. Each has its own privacy practices; review their policies. We maintain a list of core subprocessors and may update integrations; material changes will be reflected in our documentation or via notice consistent with Section 17 below.

14. Processor/Service Provider Terms (Merchants)

When acting as a processor/service provider, we: (i) process Personal Information only on your documented instructions; (ii) implement appropriate security; (iii) assist with privacy requests and security incidents; (iv) delete or return Personal Information at the end of services (subject to legal retention); and (v) **do not sell or share** the Personal Information, nor combine it for cross-context advertising.

15. Non-Custodial & Security Notice

GotSOL is **non-custodial**: we do not hold assets or private keys. **Privy** provides wallet management/authentication; your use of Privy is subject to Privy's policies. We do not control Privy and cannot access your private keys.

CRITICAL SECURITY WARNING – NO PROFESSIONAL AUDITS:

- **Anchor Program:** GotSOL's Anchor program has **not** been professionally/officially audited by third-party security firms.
- **Frontend Application:** GotSOL's frontend has **not** been professionally/officially audited for security vulnerabilities.
- **Unaudited Code Risk:** Using unaudited smart contracts/applications carries significant security risks.
- **No Security Guarantees:** We make no representations or warranties about the security, safety, or reliability of unaudited code.
- **Use at Your Own Risk:** Unaudited code may contain bugs/vulnerabilities that could result in loss of funds.

16. De-Identified & Aggregated Data

We may create and use **de-identified** or **aggregated** data that cannot reasonably be linked to you for analytics, research, and improvement. We commit to **maintain** and **use** such data in de-identified form and **not** to attempt re-identification.

17. Changes to This Policy

We may update this Policy to reflect changes in law, technology, or our practices. We will post the updated Policy with a new Effective Date and, where required, provide additional notice or seek consent. Your continued use after the Effective Date constitutes acceptance of the updated Policy.

18. Contact Us

- **Email:** gotsol-biz@protonmail.com
- **Postal:** []

US State-Specific Notice (CA, VA, CO, CT, UT, etc.)

Categories Collected (last 12 months): identifiers; account/auth; commercial data; internet/usage; wallet/transaction metadata; approximate geolocation; support content; limited inferences.

Purposes: Section 3.

Disclosures for Business Purposes: service providers (hosting, auth, DB, analytics), integration partners, compliance/safety, corporate events.

Sale/Sharing: We do **not sell** Personal Information for money. Certain analytics/ads (if used) may constitute “**sharing**” under CPRA—opt out via our banner or **GPC**.

Sensitive Personal Information: we do **not** intentionally collect SPI except where provided for KYC/compliance; we use SPI only for limited operational/legal purposes and do not use it to infer characteristics.

Consumer Rights: know/access, correct, delete, portability, opt-out of sale/sharing, limit SPI, non-discrimination. **Authorized agent** requests allowed with proper authorization.

Verification/Response: verified within statutory timelines (e.g., **45 days** in CA, extendable).

Appeals: if we deny your request, you may **appeal** by replying to our decision email with “Appeal” in the subject; we’ll respond per applicable law.