STATE OF LOC NATION GLOBAL PUBLIC BENEFIT CORPORATION

Privacy Policy

Website, Loan and Grant Platform, LND Network, and Back-End Software Services

Effective: September 1, 2026 | Version 1.1

U.S./Georgia launch draft | Users 18 and older | Separate affirmative clickwrap consents

1. Scope and Who We Are

This Privacy Policy explains how State of Loc Nation Global Public Benefit Corporation ("SOLN GPBC," "SOLN," "we," "us," or "our") collects, uses, discloses, retains, and protects personal information through https://stateoflocnation.com, the SOLN loan and grant application platform, LND accounts and transaction tools, merchant and institutional portals, and related support and back-end software services (collectively, the "Services").

SOLN administers the Services within the SOLN Sovereign Polity and its public-benefit program jurisdiction serving underfunded, unrepresented, and historically redlined persons, businesses, institutions, and communities nationally and globally. This jurisdictional framework governs SOLN program identity, community-priority criteria, internal administration, and public-benefit mission; each product and transaction is also administered in accordance with the applicable law identified in its governing agreement.

This Policy applies to applicants, borrowers, grant applicants and recipients, LND users, merchants, business representatives, institutional partners, website visitors, and support contacts. A separate financial privacy notice may apply when SOLN GPBC acts as a financial institution or provides a covered financial product or service.

2. Information We Collect

Category	Examples
Identity and contact	Name, date of birth, mailing address, email, telephone number, account credentials, government identifiers, and identity-verification results.
Application and eligibility	Requested product, amount, purpose, redlined/underfunded community eligibility information, household or business information, grant criteria, and supporting documents.
Financial and credit	Income, employment, bank account and payment information, assets, obligations, transaction history, credit information, loan performance, and repayment activity.
LND and USD activity	LND account identifier, issuance, transfers, QR activity, merchant acceptance, balances, conversion requests, USD settlement instructions, and reconciliation records.
Business and institutional	Entity name, formation and tax information, beneficial owners or controllers, authorized users, contracts, program records, and compliance materials.

Device and usage	IP address, browser, device identifier, timestamps, pages, clicks, session logs, cookies, approximate location, and security events.
Communications	Emails, calls, chats, complaints, support requests, surveys, preferences, and records of notices and consent.
Sensitive data when required	Government identifiers, account credentials, precise location, biometric or selfie-derived verification data, and other information treated as sensitive under applicable law.

3. Sources of Information

- Directly from you or your authorized representative.
- From participating merchants, sponsors, employers, community organizations, institutions, and service providers.
- From identity, fraud, sanctions, KYC/AML, payment, banking, credit-reporting, and data-verification providers where legally permitted.
- From public records, public websites, government sources, and information you direct another party to provide.
- Automatically from devices, browsers, cookies, and platform logs.

4. How We Use Information

- Provide, personalize, administer, and support the Services.
- Verify identity, eligibility, authority, and account ownership; prevent fraud, manipulation, unauthorized transfers, and security incidents.
- Process loan and grant applications; underwrite, approve, decline, document, disburse, service, collect, reconcile, and close accounts or awards.
- Create and maintain LND and USD subledgers, transaction records, statements, receipts, QR functions, and settlement evidence.
- Comply with applicable consumer-finance, privacy, tax, accounting, sanctions, anti-money-laundering, recordkeeping, reporting, and legal obligations.
- Evaluate program performance, community impact, accessibility, product quality, and risk.
- Communicate notices, decisions, statements, updates, service messages, and—where permitted—marketing.
- Protect rights, safety, property, systems, users, partners, and the public; investigate disputes and enforce agreements.

5. Automated Processing and Credit Decisions

SOLN GPBC may use rules, models, and automated tools to verify identity, screen applications, detect fraud, prioritize review, or support eligibility and underwriting. Where applicable law requires human review, specific reasons for adverse action, an opportunity to correct information, or another safeguard, SOLN GPBC will provide that process. Automated tools must not be used to discriminate on a prohibited basis.

6. When We Disclose Information

- Service providers and processors that support hosting, identity verification, fraud prevention, communications, analytics, payments, banking, servicing, collections, document generation, security, and professional advice.
- Credit bureaus or data providers only with a lawful permissible purpose and required notices or authorization.
- Sponsors, merchants, institutions, or program partners as necessary to evaluate, deliver, monitor, reconcile, and report on a program, subject to contractual and legal limits.
- Government, regulators, courts, law enforcement, auditors, insurers, or other parties when required or permitted by law or necessary to protect rights and safety.
- A successor or transaction participant in a merger, financing, reorganization, asset transfer, or similar event, subject to appropriate safeguards.
- Other recipients at your direction or with your consent.

7. Sale, Sharing, and Targeted Advertising

SOLN GPBC does not sell personal information for money. Before launch, SOLN GPBC must configure cookie and advertising tools so that any activity considered a "sale," "sharing," or targeted advertising under applicable state law is either disabled or supported by required notice and opt-out controls. We do not use sensitive personal information to infer characteristics for advertising.

8. Financial Privacy and Information Sharing

Where the Gramm-Leach-Bliley Act or another financial privacy law applies, SOLN GPBC will provide the applicable initial and annual privacy notices, honor required opt-out rights, limit redisclosure and reuse, and maintain safeguards for customer information. This online Policy does not replace a required model financial privacy notice.

9. Cookies and Similar Technologies

We may use essential cookies for login, security, preferences, and service operation; analytics cookies to understand performance; and optional technologies only after any consent required by law. Users must be offered a clear way to manage nonessential cookies where required. Disabling essential technologies may prevent account access or transaction completion.

10. Data Retention

We retain information for the period reasonably necessary for the purposes described above, including account administration, loan servicing, grant closeout, reconciliation, audits, disputes, fraud prevention, legal compliance, and enforcement. Retention periods vary by record type and legal obligation. Data no longer required will be deleted, de-identified, or securely archived according to an approved retention schedule.

11. Security

We use administrative, technical, and physical safeguards designed to protect personal information, including role-based access, multifactor authentication, encryption where appropriate, segregation of duties, logging, vendor oversight, incident response, backup, and reconciliation. No method is completely secure; users must protect credentials and promptly report suspected compromise.

12. Your Choices and Rights

- Access or update account information.
- Request access, correction, deletion, portability, restriction, or appeal where applicable.
- Opt out of marketing communications; service and legal notices will continue.
- Manage nonessential cookies and state-law opt-outs where available.
- Withdraw consent prospectively when processing depends on consent.
- Dispute inaccurate credit or transaction information through the provided channel.
- Withdraw consent to electronic delivery as described in the Electronic Records Consent, understanding that paper delivery or account limitations may apply.

Submit privacy requests to info@stateoflocnation.com. We may verify identity and authority before responding. Authorized agents must provide proof of authority. We will not unlawfully discriminate against a person for exercising privacy rights.

13. Children

The Services are intended for persons 18 years of age or older. We do not knowingly collect personal information from children under 13 through a child-directed service. If we learn that we collected such information without legally valid authorization, we will delete it as required.

14. International Users

The initial launch is designed for the United States, with Georgia as the operating base. Before offering Services in another country, SOLN GPBC will issue any required regional notice, establish a lawful transfer mechanism, identify the local controller or representative where required, and complete country-specific legal and security review.

15. Google User Data and Google Workspace APIs

Application identity. The Google-connected application covered by this Policy is SOLN Ledger Control, a Google Apps Script ledger and administrative-control application developed and operated by State of Loc Nation Global Public Benefit Corporation.

Google data accessed. Based on the current application configuration, SOLN Ledger Control accesses the signed-in user’s Google account email address for identity, role authorization, and audit attribution, and accesses the Google Spreadsheet to which the script is bound, including its sheets, cells, transaction records, journal entries, reconciliation records, account and party records, configuration values, and audit logs. The application does not access Gmail message contents, Google Calendar, Google Contacts, Google Photos, or Drive files outside the spreadsheet to which the application is bound.

How Google data is used. Google account and spreadsheet data are used only to authenticate authorized users; enforce maker-checker and role controls; create, review, approve, reconcile, and audit ledger entries; maintain account, party, payment, journal, and configuration records; detect duplicate or unauthorized activity; and provide the user-facing functions requested through the application. Google user data is not used to determine creditworthiness, make lending or grant-eligibility decisions, serve advertising, create advertising profiles, or build unrelated databases.

Sharing and transfer. SOLN GPBC does not sell Google user data, provide it to data brokers or information resellers, or transfer it for advertising, lending, or creditworthiness purposes. Google user data may be processed by Google as the application platform and by service providers acting for SOLN GPBC only as necessary to operate, secure, support, or audit the application, or disclosed when required by applicable law. Access is limited to authorized personnel and processors with a need to perform those functions.

Protection. SOLN GPBC protects Google user data through Google authentication, role-based authorization, least-privilege access, segregation of duties, audit logging, transaction identifiers, duplicate controls, reconciliation, and account-access review. Encryption and platform security supplied by Google apply to data in transit and at rest within Google Workspace; SOLN GPBC applies its own administrative safeguards to application access and use.

Retention, deletion, and revocation. Google user data and ledger records are retained only as long as needed to operate the application, maintain transaction and audit integrity, resolve disputes, and meet legal, accounting, security, and recordkeeping obligations. A user may request deletion of eligible personal information by emailing info@stateoflocnation.com and may revoke the application's Google account access through the security settings of the user's Google Account. Revocation stops future access but does not require deletion of transaction, audit, or compliance records that SOLN GPBC must lawfully retain.

Google API Limited Use. SOLN GPBC's use and transfer to any other application of information received from Google APIs will adhere to the Google API Services User Data Policy, including the Limited Use requirements. Google Workspace API data is not used to develop, improve, or train generalized or non-personalized artificial-intelligence or machine-learning models.

16. Changes to this Policy

We may update this Policy. The posted version will show its effective date. Material changes will be presented through a prominent notice and, when required, a new affirmative consent. Historical versions and acceptance records will be retained.

17. Contact Us

State of Loc Nation Global Public Benefit Corporation
Privacy Office
Mailing address: 8 The Green, Dover, Delaware 19901
Website: https://stateoflocnation.com
Email: info@stateoflocnation.com
Phone: 770-647-3915

Appendix A — Required Privacy-Related Clicks

Screen / trigger	Required text beside the control	Evidence to retain
Account creation	☐ I acknowledge that I received and reviewed the Privacy Policy.	Policy version, user ID, UTC timestamp, IP/device data, checkbox state, rendered text or hash.

Electronic records	☐ I consent to receive records and disclosures electronically and confirm I can access, download, and retain them.	Separate E-SIGN consent version, hardware/software disclosure, test/confirmation, timestamp.
Credit report, if used	☐ I authorize SOLN GPBC and its service providers to obtain and use consumer reports for my application and account as permitted by law.	Exact authorization, permissible purpose, bureau/provider, timestamp, withdrawal limits.
Sensitive identity data	☐ I consent to the collection and use of my selfie, identity document, and related verification data for identity and fraud prevention.	Notice version, purpose, retention disclosure, vendor, affirmative consent.
Marketing	☐ I agree to receive optional marketing communications. I may unsubscribe at any time.	Channel-specific opt-in, source, timestamp; never prechecked.
Material policy change	☐ I acknowledge the updated Privacy Policy dated [DATE].	Old/new versions, change notice, user action, timestamp.

Appendix B — Pre-Publication Data Map Gate

Do not publish this Policy until the product owner confirms the following against the actual system:

- Every field collected on every form and every source supplying it.
- Every vendor and partner receiving data, its role, contract, location, retention, and deletion path.
- Whether credit reports, bank data, biometrics, precise location, cookies, advertising tools, or automated decisions are actually used.
- Record-retention periods by loan, grant, LND, payment, identity, security, complaint, tax, and marketing record.
- Applicable state privacy supplements and consumer-request workflow.
- Incident-response contact, verified mailing address, and financial privacy notice.

Implementation References

- Federal E-SIGN Act, 15 U.S.C. § 7001 et seq.
- Georgia Uniform Electronic Transactions Act, O.C.G.A. § 10-12-1 et seq.
- Gramm-Leach-Bliley Act privacy and safeguards requirements and implementing rules, where applicable.
- Fair Credit Reporting Act and Regulation V, where consumer reports are used or furnished.
- Equal Credit Opportunity Act and Regulation B; Truth in Lending Act and Regulation Z, where applicable.
- FTC COPPA Rule for any future child-directed service.