AIConsensusAudit.com Privacy Policy

Effective Date: July 6, 2026
Website: AIConsensusAudit.com
Token: $AICA. This Privacy Policy explains how **[Company Legal Name]**, doing business as **AI Consensus Audit**, **AIConsensusAudit.com**, and related brands, collects, uses, stores, shares, and protects information when you access or use our website, smart-contract scanning tools, AI audit engine, APIs, reports, wallet-based payment features, token-related functionality, and related services. For purposes of this Privacy Policy, **"AI Consensus Audit," "we," "us," or "our"** refers to **[Company Legal Name]**. **"User," "you," or "your"** refers to any person or entity that accesses or uses the Services. By using the Services, connecting a wallet, submitting code, purchasing a scan, using $AICA, or otherwise interacting with AIConsensusAudit.com, you agree to the practices described in this Privacy Policy. If you do not agree with this Privacy Policy, do not use the Services.

---

1. Scope of This Privacy Policy

This Privacy Policy applies to information we collect through:

- **AIConsensusAudit.com**
- **Smart-contract scan submissions**
- **Code upload or paste features**
- **Repository integrations**
- **AI-generated audit reports**
- **Wallet connections**
- **Crypto payments**
- **$AICA-related functionality**
- **API access**
- **Customer support**
- **Analytics and security tools**
- **Email or other communications with us**

This Privacy Policy does not apply to third-party websites, wallets, blockchain networks, exchanges, payment processors, AI model providers, repository platforms, or other third-party services that we do not control.

---

2. Information We Collect

We may collect several categories of information depending on how you use the Services.

2.1 Information You Provide Directly

You may provide information to us when you:

- Submit code for a scan
- Paste a smart contract into the platform
- Upload files
- Link a repository
- Purchase a scan
- Contact support
- Request API access
- Join a waitlist
- Subscribe to updates
- Submit bug reports
- Participate in grants, incentives, or research programs
- Communicate with us by email, forms, chat, or social channels

This information may include:

- **Name**
- **Email address**
- **Company or project name**
- **Telegram, Discord, X/Twitter, GitHub, or other handles**
- **Billing or payment-related details**
- **Support messages**
- **Project descriptions**
- **Smart-contract code**
- **Repository links**
- **Documentation**
- **Protocol metadata**

- **Uploaded files**
- **API request details**
- **Any other information you choose to submit**

2.2 Code, Repository, and Scan Data

When you submit code or connect a repository, we may collect and process:

- **Smart-contract source code**
- **Repository files**
- **File names and paths**
- **Compiler versions**
- **Dependencies**
- **Configuration files**
- **Protocol documentation**
- **README files**
- **Comments inside code**
- **Function names**
- **Contract names**
- **Modifiers**
- **State variables**
- **External call structures**
- **Architecture information**
- **Generated audit reports**
- **Risk scores**
- **Vulnerability findings**
- **Suggested fixes**
- **Scan history**
- **Re-scan results**

You are responsible for ensuring that you have the right to submit any code, repository, documentation, or related materials to the Services. You should not submit private keys, seed phrases, passwords, production secrets, confidential credentials, or sensitive information that is not necessary for the scan.

2.3 Wallet and Blockchain Information

If you connect a wallet, pay with cryptocurrency, use $AICA, or otherwise interact with blockchain-based features, we may collect or process:

- **Public wallet address**
- **Transaction hashes**
- **Payment token used**
- **Payment amount**
- **Network or chain used**
- **Timestamp of transaction**
- **Smart-contract interaction data**
- **On-chain payment confirmation**
- **Token-gating or token-payment status**
- **Gas/network-related metadata**

Blockchain transactions are public by nature. Information recorded on public blockchains may be visible to anyone and may not be deleted or modified by us. We do not collect or store your private keys, seed phrases, or wallet recovery phrases. You should never provide them to us.

2.4 Payment Information

For crypto payments, we may collect transaction-related information such as:

- **Wallet address**
- **Payment amount**
- **Token used**
- **Network**
- **Transaction hash**
- **Payment status**
- **Checkout session data**

If we support third-party payment processors in the future, those processors may collect payment information under their own privacy policies. We do not control third-party payment providers, wallet providers, exchanges, bridges, or blockchain networks.

2.5 API and Usage Information

When you use our website, APIs, or developer tools, we may collect technical and usage information, including:

- **IP address**
- **Browser type**
- **Device type**
- **Operating system**
- **Referring URLs**
- **Pages viewed**
- **Session timestamps**
- **API endpoints accessed**
- **Request and response metadata**
- **Rate-limit data**
- **Error logs**
- **Authentication events**
- **Scan volume**
- **Feature usage**
- **Performance data**

This information helps us operate, secure, debug, and improve the Services.

2.6 Cookies and Similar Technologies

We may use cookies, pixels, local storage, analytics tools, and similar technologies to:

- Remember user preferences
- Maintain sessions
- Improve website functionality
- Analyze traffic
- Detect abuse
- Prevent fraud
- Measure product performance
- Improve user experience

You may be able to control cookies through your browser settings. Disabling cookies may affect some platform features. If legally required, we may provide a cookie consent banner or preference center.

2.7 Information From Third Parties

We may receive information from third parties, including:

- **Wallet providers**
- **Blockchain analytics tools**
- **Repository platforms**
- **Cloud infrastructure providers**
- **AI model providers**
- **Payment processors**
- **Security vendors**
- **Analytics providers**
- **Customer support tools**
- **Public blockchain data**
- **Public websites and open-source repositories**

This information may be combined with information we collect directly.

---

3. How We Use Information

We may use collected information to:

- **Provide the Services**
- **Run AI-powered smart-contract scans**
- **Generate audit reports**
- **Process payments**
- **Verify $AICA payment eligibility**
- **Provide the preferred $AICA scan rate**
- **Create and manage user sessions**
- **Provide API access**
- **Operate repository integrations**

- **Perform continuous re-scans**
- **Debug platform issues**
- **Improve audit quality**
- **Improve AI prompts, workflows, and scoring logic**
- **Detect and prevent abuse**
- **Protect platform security**
- **Respond to support requests**
- **Communicate with users**
- **Analyze platform usage**
- **Comply with legal obligations**
- **Enforce our Terms of Service**
- **Prevent fraud, spam, attacks, or unauthorized use**
- **Maintain records of transactions and scans**
- **Develop new features**
- **Support continuous development of the AI Consensus Audit engine**

We may also use aggregated, anonymized, or de-identified data to improve the Services, evaluate model performance, generate statistics, or conduct internal research.

---

4. AI Processing and Model Providers

AI Consensus Audit uses AI systems and automated analysis to review smart-contract code and generate reports. To provide the Services, we may process Submitted Materials through:

- **Internal AI systems**
- **Third-party AI model providers**
- **Cloud-based AI infrastructure**
- **Code-analysis tools**
- **Security-analysis pipelines**
- **Model orchestration systems**

Submitted code, prompts, scan context, and related materials may be transmitted to or processed by third-party AI providers as necessary to provide the scan. We use commercially reasonable efforts to work with reputable providers and configure systems appropriately. However, you should not submit code or materials that you are not authorized to share. Where available, we may configure AI providers not to use submitted data for training their general models. However, provider practices may vary, and their services may be governed by separate terms and policies.

5. How We Share Information

We do not sell your personal information in the ordinary sense of exchanging it for money. However, we may share information with service providers and partners as necessary to operate the Services.

5.1 Service Providers

We may share information with third-party service providers that help us operate the platform, including:

- **AI model providers**
- **Cloud hosting providers**
- **Database providers**
- **Analytics providers**
- **Security vendors**
- **Wallet and blockchain infrastructure providers**
- **Payment processors**
- **Repository integration providers**
- **Email providers**
- **Customer support platforms**
- **Logging and monitoring tools**
- **Legal, compliance, and professional advisors**

These providers may process information on our behalf or under their own policies, depending on the relationship and service.

5.2 Blockchain Networks

If you interact with blockchain features, certain information will be publicly visible on-chain, including wallet addresses, transaction hashes, payment amounts, and token transfers. We cannot control or delete information recorded on public blockchains.

5.3 Legal and Compliance

We may disclose information if we believe it is necessary to:

- Comply with applicable law
- Respond to lawful requests
- Cooperate with law enforcement or regulators
- Enforce our Terms of Service
- Protect our rights, users, platform, or property
- Prevent fraud, abuse, security threats, or illegal activity
- Investigate suspected violations
- Defend against claims or legal proceedings

5.4 Business Transfers

If we are involved in a merger, acquisition, financing, reorganization, sale of assets, bankruptcy, or similar transaction, information may be transferred as part of that transaction.

5.5 With Your Direction or Consent

We may share information when you direct us to do so or give us consent, such as when you connect a repository, request support, authorize an integration, or share a report with another party.

---

6. Aggregated and De-Identified Data

We may create aggregated, anonymized, or de-identified data from information collected through the Services. We may use this data for:

- **Improving scan quality**
- **Benchmarking system performance**
- **Measuring model accuracy**
- **Analyzing vulnerability trends**
- **Improving platform reliability**
- **Research and development**
- **Product analytics**
- **Marketing statistics**

We will not intentionally use aggregated or de-identified data to identify you.

---

7. Data Retention

We retain information for as long as reasonably necessary to provide the Services, comply with legal obligations, resolve disputes, enforce agreements, prevent abuse, maintain security, improve the platform, and support business operations. Retention periods may vary depending on the type of information. Examples:

- **Scan reports** may be retained for user access, support, audit history, and re-scan functionality.
- **Code submissions** may be retained for scan delivery, debugging, abuse prevention, and service improvement.
- **Payment records** may be retained for accounting, tax, fraud prevention, and legal compliance.
- **Wallet and transaction data** may remain publicly available on blockchains indefinitely.
- **Logs and analytics data** may be retained for security, debugging, and performance monitoring.

You may request deletion of certain information as described below. However, we may retain information where required or permitted by law, where necessary for legitimate business purposes, or where deletion is not technically feasible, including public blockchain records.

---

8. Data Security

We use commercially reasonable technical, administrative, and organizational measures designed to protect information. These measures may include:

- **Access controls**
- **Encryption in transit**
- **Secure cloud infrastructure**
- **Monitoring and logging**
- **Credential management**
- **Permission controls**
- **Abuse detection**
- **Security reviews**
- **Limited internal access**
- **Vendor review processes**

However, no system is perfectly secure. We cannot guarantee that information will never be accessed, disclosed, altered, or destroyed by unauthorized parties. You are responsible for maintaining the security of your wallets, private keys, API keys, repository permissions, credentials, devices, and accounts.

---

9. Your Privacy Choices

Depending on your jurisdiction and how you use the Services, you may have certain rights regarding your personal information. These may include the right to:

- **Access personal information**
- **Correct inaccurate information**
- **Request deletion**
- **Object to certain processing**
- **Restrict certain processing**
- **Request portability**
- **Withdraw consent where processing is based on consent**
- **Opt out of certain communications**
- **Lodge a complaint with a regulator**

To exercise privacy rights, contact us at:**[Insert Privacy Email]**We may need to verify your identity before processing requests. Certain information may not be deleted if retention is necessary for legal compliance, security, fraud prevention, dispute resolution, platform integrity, accounting, tax purposes, or blockchain immutability.

---

10. Email and Communications

If you provide your email address, we may use it to send:

- **Service messages**
- **Scan updates**
- **Payment confirmations**
- **Security notices**
- **Support responses**
- **Product updates**
- **API notices**
- **Policy updates**
- **Marketing communications, where permitted**

You may opt out of marketing emails by following unsubscribe instructions. You may still receive transactional or service-related messages.

---

11. Children’s Privacy

The Services are not intended for children. You must be at least **18 years old** or the age of majority in your jurisdiction to use the Services. We do not knowingly collect personal information from children. If we learn that we have collected personal information from a child, we may delete it.

---

12. International Users

AIConsensusAudit.com may be operated from and use infrastructure located in multiple jurisdictions. By using the Services, you understand that your information may be transferred to, stored in, or processed in countries other than your country of residence. These countries may have data protection laws different from those in your jurisdiction. Where required, we use appropriate safeguards for international data transfers.

---

13. European Economic Area, United Kingdom, and Similar Jurisdictions

If you are located in the European Economic Area, United Kingdom, Switzerland, or another jurisdiction with similar data protection laws, we process personal information based on one or more legal bases, including:

- **Performance of a contract:** to provide scans, reports, payments, API access, and related Services.
- **Legitimate interests:** to operate, secure, improve, and develop the platform; prevent abuse; analyze usage; and support users.
- **Consent:** where required for cookies, marketing, or optional processing.
- **Legal obligations:** to comply with applicable laws, tax, accounting, sanctions, and regulatory requirements.

You may have rights under applicable data protection laws, including access, correction, deletion, objection, restriction, portability, and complaint rights. To exercise rights, contact:**[Insert Privacy Email]**

---

14. California Privacy Notice

If you are a California resident, you may have rights under the California Consumer Privacy Act, as amended, or similar California privacy laws. Depending on applicability, these rights may include:

- **Right to know what personal information we collect**
- **Right to access personal information**
- **Right to delete personal information**
- **Right to correct inaccurate personal information**
- **Right to opt out of sale or sharing, where applicable**
- **Right to limit use of sensitive personal information, where applicable**
- **Right not to be discriminated against for exercising privacy rights**

We do not sell personal information in the ordinary sense of exchanging it for money. However, some analytics or advertising technologies may be considered “sharing” under certain privacy laws. If applicable, we will provide appropriate opt-out mechanisms. To submit a California privacy request, contact:**[Insert Privacy Email]**

---

15. Do Not Track

Some browsers transmit “Do Not Track” signals. Because there is no uniform standard for responding to these signals, we may not respond to them unless required by law.

---

16. Sanctions, Compliance, and Abuse Prevention

We may process information, including wallet addresses, IP addresses, transaction data, and usage patterns, to detect and prevent:

- **Sanctions violations**
- **Fraud**
- **Abuse**
- **Unauthorized access**
- **Payment misuse**
- **Malicious submissions**
- **Security attacks**
- **Terms of Service violations**
- **Illegal or harmful activity**

We may use third-party tools, public blockchain data, and compliance vendors for these purposes. We may restrict or deny access to users, wallets, transactions, jurisdictions, or activity that we determine creates legal, security, operational, or compliance risk.

---

17. Public Reports and User Sharing

By default, scan reports are intended for the user who submitted the scan. If you choose to publish, export, forward, or share a report, you are responsible for that disclosure. We are not responsible for third-party use, interpretation, redistribution, or reliance on reports that you choose to share. If public report features are introduced, additional settings or terms may apply.

---

18. Open-Source and Public Code

If you submit open-source or publicly available code, we may process it in the same way as other Submitted Materials. Public availability of code does not necessarily mean the related scan, report, metadata, or user account information is public. However, you should assume that public code may already be accessible to third parties outside our platform.

---

19. Sensitive Information

You should not submit sensitive personal information unless necessary. This includes:

- Government identification numbers
- Health information
- Biometric information
- Financial account credentials
- Private keys
- Seed phrases
- Passwords
- API secrets
- Confidential credentials
- Personal data embedded in code or documentation

If you include sensitive information in Submitted Materials, you do so at your own risk. We may delete or restrict materials containing sensitive information where feasible.

---

20. Repository Integrations

If you connect GitHub, GitLab, Bitbucket, or another repository platform, we may access repository content according to the permissions you authorize. We may process:

- Repository names
- Branches
- Commits
- Pull requests
- Files
- Code diffs
- Dependency files
- Documentation
- Metadata
- Webhook events

You may revoke repository access through the third-party platform or through AIConsensusAudit.com where available. We are not responsible for permissions you grant through third-party repository providers.

---

21. API Keys and Developer Access

If we provide API access, we may collect and process:

- API keys
- Authentication tokens
- Request metadata
- Rate-limit data
- Usage volume
- Error logs
- Scan submissions
- Account or project identifiers

You are responsible for securing your API keys and ensuring they are not exposed in public repositories, client-side code, logs, or unsecured environments. We may suspend API access if we detect abuse, compromised credentials, excessive usage, or security risk.

---

22. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. If we make material changes, we may notify users by posting the updated policy on the website, updating the effective date, sending an email where appropriate, or using other reasonable methods. Your continued use of the Services after an updated Privacy Policy becomes effective means you accept the revised policy. If you do not agree with the updated Privacy Policy, stop using the Services.

---

23. Contact Us

If you have questions, requests, or concerns about this Privacy Policy or our privacy practices, contact us at: **AI Consensus Audit**
Website: **AIConsensusAudit.com**
Company: **[Company Legal Name]**
Privacy Email: **[Insert Privacy Email]**
Support Email: **[Insert Support Email]**
Address: **[Insert Company Address]**

Suggested Short Footer Privacy Notice

You can also use this in the site footer:**AIConsensusAudit.com processes submitted code, wallet addresses, transaction data, usage data, and related materials to provide AI-assisted smart-contract scans, generate reports, process payments, prevent abuse, and improve the platform. Do not submit private keys, seed phrases, passwords, or code you are not authorized to share.**
