

INVO NETWORK

PRIVACY POLICY

Effective Date: October 13, 2026

This Privacy Policy explains how Invo Tech, Inc. and its affiliates ("INVO," "we," "us," or "our") collect, use, share, and protect personal information when you use the INVO platform, our websites, applications, APIs, and related services (collectively, the "Service").

This Privacy Policy applies to:

- Players who use the Service to purchase, transfer, or use Virtual Currency in supported Games
- Developers who integrate with the Service
- Creators and other payees whom INVO verifies and pays through a Developer's creator program ("Payees")
- Visitors to our websites and other Service touchpoints

If you are located in the European Economic Area, the United Kingdom, Switzerland, California, or another jurisdiction with specific privacy rights, please see the jurisdiction-specific sections below.

Contents

1. Quick Summary
2. Information We Collect
3. How We Use Information
4. Legal Bases for Processing (EU/UK/EEA Users)
5. How We Share Information
6. International Data Transfers
7. Data Retention
8. Children and Teens
9. SMS, Phone, and Communications
10. Cookies and Tracking Technologies
11. Security
12. Your Privacy Rights
13. EU/UK/EEA Users (GDPR / UK GDPR)
14. California Residents (CCPA/CPRA)
15. Other U.S. State Privacy Laws
16. Other Jurisdictions
17. Third-Party Services and Links
18. Changes to This Policy
19. How to Contact Us
20. Payees: How to Exercise Your Rights

1. Quick Summary

Here is the short version of how we handle your information:

- We collect information you provide (account details, contact info, identity verification), information generated by your use of the Service (transactions, balances, device data), and limited information from third parties (Game developers, payment processors, fraud and identity verification providers).
- We use this information to operate the Service, process transactions, prevent fraud, comply with legal obligations, communicate with you, and improve the Service.
- We do NOT sell your personal information for money. We share information with service providers, Game developers (limited), our Payment Processor, and as required by law.
- We do NOT process or sell sensitive personal information for cross-context behavioral advertising.
- You have rights over your information, including access, correction, deletion, and (in certain jurisdictions) portability and objection.
- If you are in the EU, UK, EEA, or California, you have additional rights described below.
- If you are under 18, additional protections apply, and a parent or guardian must consent to your use of the Service.

2. Information We Collect

2.1 Information You Provide

When you create an account or use the Service, you may provide:

- Account information: name, email address, phone number, username, password, date of birth
- Profile information: display name, avatar, language and region preferences, communication preferences
- Guardian information (for users under 18): parent or guardian name, email address, phone number, and consent records
- Identity verification information (where required): government-issued ID, date of birth, address, and other documentation needed for KYC, sanctions screening, or withdrawal verification
- Payee information: if you are a Payee, your legal name, business name and type, date of birth, country of citizenship, address, email address, government-issued identification and images of it, taxpayer identification number and tax certification (such as IRS Form W-9 or W-8), for a business its formation details and the people who own or control it, bank account and routing details, and your acceptance of the

INVO Payee Terms and of electronic delivery of tax forms. You provide this to us directly on INVO's pages.

- Communications: messages you send to support, dispute submissions, and other inquiries
- Survey and feedback responses, if you choose to provide them

2.2 Information We Generate From Your Use

As you use the Service, we automatically collect:

- Transaction records: Virtual Currency purchases, transfers, sends, item purchases, withdrawals, and balance changes
- Account activity: logins, sessions, device information, IP address, time zone, and approximate location derived from IP
- Device and technical data: device type, operating system, browser type, app version, language settings, and unique device identifiers
- Usage data: features you access, pages or screens you view, click and tap events, error reports, and performance data
- Consent records: SMS one-time-passcode verifications, guardian approvals, phone-share approvals, and cross-Game wallet bindings
- Fraud and security signals: device fingerprints, behavioral patterns, velocity data, risk scores, and suspicious-activity flags

2.3 Information We Receive From Others

We may receive information from:

- Payment Processor: payment method type, transaction status, settlement confirmations, chargeback notifications, and KYC verification status (we do not receive full card numbers or bank credentials, only tokens and metadata)
- Game developers: in-Game Player identifiers, Game-related events relevant to your INVO transactions, and information needed to operate the cross-Game features you use
- Developers operating creator programs: a Payee's name, email address, country and type, the identifier the Developer uses for the Payee, and the amounts the Developer instructs us to pay
- Identity and fraud verification providers: results of identity, sanctions, and fraud checks, including PEP (politically exposed person) screening where required
- SMS, email, and authentication providers: delivery status, bounces, and authentication outcomes
- Analytics and infrastructure providers: aggregated and pseudonymized usage and performance data
- Public sources, government registries, and sanctions lists, where lawful

2.4 Information We Do Not Collect

We do not collect or store: full credit card or debit card numbers, bank account credentials, or wallet private keys. These are held by the Payment Processor and its subcontracted processors, not by INVO.

2.5 Sensitive Information

We do not intentionally collect sensitive personal information beyond what is necessary for identity verification, sanctions screening, fraud prevention, and compliance with applicable law. Where we collect such information, we apply additional protections and limit access to authorized personnel.

2.6 Payees

If you are a Payee, we collect the information in Sections 2.1 and 2.3 to verify who you are, to check you against sanctions and restricted-party lists, to meet our tax reporting obligations, to prevent fraud, and to pay you. INVO contacts you directly, names the Developer whose creator program you joined, and is the company that verifies and pays you. This Privacy Policy describes how we handle your information.

3. How We Use Information

We use personal information for the following purposes:

3.1 Operating the Service

- Creating and maintaining your account
- Processing Virtual Currency purchases, transfers, sends, items, and withdrawals
- Maintaining balance records and transaction history
- Implementing consent flows (SMS one-time-passcodes, guardian approvals, phone-share approvals)
- Providing customer support and resolving disputes
- Managing inactive balances under applicable law

3.2 Security and Fraud Prevention

- Detecting, preventing, and investigating fraud, abuse, and security incidents
- Verifying identity and authenticating sessions
- Enforcing our terms, policies, and applicable law
- Conducting sanctions and PEP screening
- Maintaining audit trails for compliance

3.3 Legal and Regulatory Compliance

- Complying with KYC/AML and sanctions obligations through our Payment Processor and verification providers
- Meeting tax and financial reporting requirements
- Administering unclaimed property and inactive balance laws
- Responding to lawful requests from courts, regulators, and law enforcement
- Defending legal claims and exercising legal rights

For Payees, this includes identity verification, sanctions and restricted-party screening, anti-money-laundering record keeping, collecting tax information, and issuing year-end information returns for the payments we make.

3.4 Communications

- Sending transactional notifications (account, security, transactions, disputes, inactive balance notices)
- Responding to support requests
- Sending product updates, surveys, and (where you have opted in or where permitted) marketing communications

3.5 Improving the Service

- Analyzing usage and performance
- Developing new features and improving existing ones
- Conducting research and analytics, including using aggregated or pseudonymized data
- Training internal models for fraud detection, support automation, and risk management (we do not train external AI models on your personal information without appropriate safeguards)

3.6 Aggregated and De-Identified Information

We may create aggregated, statistical, or de-identified information from personal information. We may use and share this information without restriction, provided it cannot reasonably be used to identify you.

3.7 Paying Payees

We use Payee information to verify the Payee, to screen the Payee before the first payment and periodically afterwards, to verify the Payee's bank account, to make payments to the Payee's bank account, to handle returned payments, to issue tax documents, to prevent and investigate fraud, and to keep the records the law requires. We tell the Developer whose creator program the Payee joined whether verification is complete or needs more information, and the status of each payment. We do not share a Payee's identification documents, taxpayer identification number or bank account details with the Developer.

4. Legal Bases for Processing (EU/UK/EEA Users)

If you are in the European Economic Area, the United Kingdom, or Switzerland, we rely on the following legal bases under the GDPR and UK GDPR:

4.1 Performance of Contract

Most processing is necessary to provide the Service to you, including creating your account, processing transactions, communicating with you about your account, and providing support. Without this processing, we cannot deliver the Service you have requested.

4.2 Legal Obligation

We process certain information to comply with applicable laws, including KYC/AML, sanctions, tax reporting, unclaimed property, and consumer protection laws.

4.3 Legitimate Interests

We process information for legitimate interests including: preventing fraud and abuse, securing the Service, improving the Service, defending legal claims, and conducting business operations. We balance these interests against your privacy rights and apply appropriate safeguards. You may object to processing based on legitimate interests as described in Section 13.

4.4 Consent

Where required by law (for example, certain marketing communications, optional cookies, or processing of children's data), we rely on your consent. You may withdraw consent at any time without affecting the lawfulness of processing before withdrawal.

4.5 Vital Interests and Public Interest

In rare cases, we may process information to protect vital interests (such as life or safety) or in the public interest.

5. How We Share Information

We share personal information only as described below.

5.1 Service Providers

We share information with vendors and service providers that help us operate the Service, including:

- Payment Processor and its subcontracted card and bank payment processors
- Banking partners that hold or route funds
- Accounting and bill-payment software providers, which record and pay the payouts we make, including payments to Payees

- Identity verification, document verification, bank account verification, sanctions screening and fraud prevention providers, which act on our instructions
- SMS, email, and push notification delivery providers
- Cloud infrastructure, hosting, and security providers
- Analytics and performance monitoring providers
- Customer support and ticketing platforms
- Professional advisors (legal, accounting, audit)

These providers are bound by contractual obligations to protect your information and use it only for the purposes we specify.

5.2 Game Developers

To operate cross-Game and in-Game features, we share limited information with Game developers, including: (a) your INVO Player identifier within their Game; (b) Transaction events relevant to their Game (such as Virtual Currency credits or item purchases); and (c) consent and verification status as needed to operate consent flows. Game developers do not receive your full account profile, payment information, or transaction history outside their Game, except as needed to operate cross-Game features you have used. For Payees, we share with the Developer whose creator program the Payee joined only the Payee's verification status, payment status and amounts paid.

5.3 Cross-Game Data and the WalletUser System

If you use multiple Games supported by INVO, your account may be linked across Games through a cross-Game Player identity ("WalletUser"). This allows you to transfer Virtual Currency between Games and to maintain a unified account experience. Game developers do not see other Games' Player profiles, but they may receive notice of cross-Game Transactions you initiate involving their Game.

5.4 Legal and Safety Disclosures

We may disclose information to:

- Comply with applicable law, regulation, court order, subpoena, or governmental request
- Enforce our terms and policies
- Detect, prevent, or address fraud, security, or technical issues
- Protect the rights, property, or safety of INVO, our users, or others
- Cooperate with sanctions, AML, tax, or unclaimed property authorities

5.5 Corporate Transactions

If INVO is involved in a merger, acquisition, financing, reorganization, sale of assets, or bankruptcy, your information may be transferred as part of that transaction. We will notify you of any change in the controller of your information as required by applicable law.

5.6 With Your Consent

We may share information with other parties where you direct us to do so or otherwise consent.

5.7 No Sale of Personal Information

We do not sell your personal information for money. We do not share your personal information for cross-context behavioral advertising. See Section 14 for California-specific definitions of "sale" and "share."

6. International Data Transfers

6.1 Where We Process Information

INVO is based in the United States. We and our service providers may process information in the United States, the European Economic Area, the United Kingdom, and other countries where we or our service providers operate. These countries may have data protection laws that differ from your country.

6.2 Safeguards for Transfers from EU/UK/EEA

When we transfer personal information from the European Economic Area, the United Kingdom, or Switzerland to countries that have not been deemed adequate by the European Commission or the UK Information Commissioner's Office, we rely on appropriate safeguards, including:

- Standard Contractual Clauses approved by the European Commission and (where applicable) the UK International Data Transfer Agreement or Addendum
- Other lawful transfer mechanisms permitted under applicable law

You may request a copy of the safeguards we use by contacting us as described in Section 19.

7. Data Retention

We retain personal information for as long as necessary to provide the Service, comply with our legal obligations, resolve disputes, and enforce our agreements. Specific retention periods depend on the type of information and applicable legal requirements, including:

- Account and transaction records: retained for the period required by financial, tax, and unclaimed property laws (typically several years after account closure)
- KYC and sanctions screening records: retained for the period required by applicable AML and sanctions law
- Consent records: retained for the period necessary to demonstrate compliance with consent-based processing obligations

- Fraud and security data: retained as long as necessary to detect and investigate ongoing or repeat misconduct
- Communications and support records: retained for a period appropriate to resolve and document support matters
- Marketing preferences: retained to honor your choices
- Payee identity verification, sanctions screening and consent records: retained for ten (10) years after the Payee relationship ends, or longer where applicable law requires
- Payee payment and tax records: retained for ten (10) years after the end of the tax year in which the payment was made

Information a Payee entered on our pages but never submitted is deleted when it is no longer needed. When a Payee asks us to delete their information, we delete what the law does not require us to keep and restrict the rest to the purposes for which it must be kept.

When information is no longer needed, we delete, anonymize, or de-identify it in accordance with our retention schedules.

8. Children and Teens

8.1 Minimum Age

The Service is not intended for and we do not knowingly collect personal information from children under 13. In jurisdictions that set a higher minimum age for processing children's data without parental consent (for example, parts of the European Economic Area, where the age may be 14, 15, or 16), the higher local age applies.

8.2 Users Aged 13-17

If you are between 13 and 17 (or under the applicable local minimum age), you may only use the Service with the consent and supervision of a parent or legal guardian. We require guardian approval for account creation and for certain higher-risk transactions. Parents and guardians can review, request changes to, or delete their child's account by contacting INVO support.

8.3 If We Learn a Child Has Used the Service

If we learn that we have collected personal information from a child under 13 (or under the applicable local minimum age) without proper parental consent, we will delete the information promptly and close the account. Parents and guardians who believe their child has provided personal information to us without consent should contact INVO support.

8.4 COPPA (United States)

Where the U.S. Children's Online Privacy Protection Act ("COPPA") applies, we follow COPPA's requirements for verifiable parental consent, parental access, and limitations on collection from children under 13.

8.5 Special Protections for Minors

For Players we know to be under 18, we apply additional protections, including: (a) limits on profile visibility and communications; (b) guardian approval requirements for certain Transactions; (c) restrictions on marketing communications; and (d) heightened review of unusual activity.

9. SMS, Phone, and Communications

9.1 SMS Verification and Notifications

We use SMS messages for account security and Service operations, including: one-time-passcode (OTP) verification for sign-in and Transactions, guardian approval requests, phone-share consent requests, fraud alerts, transaction confirmations, and inactive balance notifications. Standard message and data rates from your carrier may apply.

9.2 Consent to Receive SMS

By providing your phone number to INVO, you consent to receive transactional SMS messages necessary to operate the Service. These messages are not marketing. You may stop most SMS messages by replying STOP to any message, but doing so may impact your ability to use account security features and certain Transactions. We do not send marketing SMS messages without your separate, prior consent.

9.3 Email and Push Notifications

We send transactional and security email and push notifications by default. You can manage marketing email preferences through your account settings or via the unsubscribe link in our marketing emails. You cannot opt out of transactional communications necessary to operate the Service.

9.4 Phone-Share Consent System

If a phone number you provide is already associated with another INVO account, the existing phone-owner must consent to share the phone number across accounts. We use SMS to administer this consent and we record consent decisions. You may revoke phone-share approvals through your account settings.

10. Cookies and Tracking Technologies

10.1 What We Use

INVO and our service providers use cookies, local storage, SDKs, pixels, and similar technologies to operate the Service, remember your preferences, secure your account, prevent fraud, analyze usage, and improve the Service.

10.2 Categories

- Strictly necessary: required to operate the Service, including authentication, security, and consent flows
- Performance and analytics: help us understand how the Service is used and improve it
- Functional: remember your preferences and settings
- Fraud and security: help detect and prevent fraud, abuse, and unauthorized access

10.3 Your Choices

Where required by law, we obtain consent before using non-essential cookies and similar technologies. You can manage your preferences through our cookie banner (where available) and your browser or device settings. Disabling certain cookies may affect Service functionality.

10.4 Do Not Track

Our Service does not currently respond to Do Not Track browser signals because there is no industry standard for handling them. We respond to Global Privacy Control signals where required by applicable law.

11. Security

We use technical, administrative, and physical safeguards designed to protect personal information from unauthorized access, use, and disclosure. These include encryption in transit and at rest where appropriate, access controls, monitoring, security testing, employee training, and vendor due diligence.

No system is perfectly secure. You can help protect your account by using a strong unique password, enabling all available account security features, keeping your contact information current, and promptly reporting any suspected compromise to INVO support.

If we experience a security incident affecting your personal information, we will notify you and, where required, applicable authorities, in accordance with applicable law.

12. Your Privacy Rights

Subject to applicable law and identity verification, you may have the following rights with respect to your personal information:

- Access: request a copy of the personal information we hold about you
- Correction: request that we correct inaccurate or incomplete information
- Deletion: request deletion of your personal information, subject to legal exceptions
- Portability: request a copy of certain information in a portable format
- Restriction: request that we restrict processing in certain circumstances
- Objection: object to certain processing, including processing based on legitimate interests or for direct marketing

- Withdraw consent: where processing is based on consent, withdraw your consent at any time
- Lodge a complaint: complain to a privacy regulator in your jurisdiction

To exercise these rights, contact us as described in Section 19. We will respond within the timeframes required by applicable law. We may need to verify your identity before responding. Some rights have legal exceptions; we will tell you when an exception applies.

You may also have rights to limit our use of sensitive personal information and to opt out of certain disclosures, as described in the jurisdiction-specific sections below.

13. EU/UK/EEA Users (GDPR / UK GDPR)

13.1 Data Controller and Processor

Invo Tech, Inc. is the data controller for:

- your INVO account, identity, consent and verification records, and the cross-Game identity described in Section 5.3
- payment, payout and Payee records, including the information about Payees described in Sections 2.6 and 3.7
- financial and tax records for sales where INVO is the merchant of record
- fraud prevention, security and legal compliance processing described in Sections 3.2 and 3.3

Where INVO processes Player information for a Developer on the Developer's instructions, for the Developer's own Game-specific purposes, and the Developer is the seller of what the Player buys (the Open tier), the Developer is the data controller for that processing and INVO is its processor under INVO's Data Processing Addendum.

13.2 Your Rights Under GDPR / UK GDPR

If you are in the European Economic Area, the United Kingdom, or Switzerland, you have the rights described in Section 12, plus the following:

- Right to lodge a complaint with your local supervisory authority. In the EU, you can contact your country's data protection authority. In the UK, you can contact the Information Commissioner's Office (ICO) at ico.org.uk. In Switzerland, you can contact the Federal Data Protection and Information Commissioner (FDPIC)
- Right not to be subject to decisions based solely on automated processing that produce legal or similarly significant effects, except where permitted by law and with appropriate safeguards. We use automated processing for fraud detection, identity verification, and Transaction risk scoring; you may request human review of such decisions
- Right to be informed about international data transfers and the safeguards we use, as described in Section 6

13.3 EU/UK Representative

Where required by Article 27 of the GDPR or UK GDPR, we will appoint a representative in the European Union and the United Kingdom. Contact details for our representatives, where applicable, will be published in the Platform Policies.

13.4 Legal Bases (Reminder)

The legal bases on which we rely are described in Section 4.

13.5 How to Exercise Your Rights

You may exercise your GDPR/UK GDPR rights by contacting us as described in Section 19. We will respond within one month, with extensions as permitted by law for complex requests.

14. California Residents (CCPA/CPRA)

This Section provides additional information for California residents under the California Consumer Privacy Act, as amended by the California Privacy Rights Act (collectively, the "CCPA").

14.1 Categories of Information Collected

In the past 12 months, we may have collected the following categories of personal information about California residents:

- Identifiers (name, email, phone, IP address, account identifiers)
- Commercial information (transaction history, balances)
- Internet or other electronic network activity (usage data, device data)
- Geolocation (approximate location from IP)
- Audio, electronic, or similar information (support call recordings, where applicable)
- Professional or employment-related information (for Developer accounts)
- Inferences drawn from the above (for fraud detection and Service personalization)
- Sensitive personal information (government ID for KYC, account credentials, precise geolocation in limited cases)

14.2 Sources, Purposes, and Disclosures

The sources from which we collect information are described in Section 2; the purposes for which we use information are described in Section 3; and the categories of recipients with whom we share information are described in Section 5.

14.3 No Sale, No Sharing for Cross-Context Behavioral Advertising

We do not sell personal information for money. We do not share personal information for cross-context behavioral advertising as defined under the CCPA. We do not knowingly sell or share the personal information of consumers under 16.

14.4 Sensitive Personal Information

We use sensitive personal information only for purposes permitted under CCPA without additional consent (such as providing the Service, security, and fraud prevention) or with your consent where required.

14.5 Your CCPA Rights

California residents have the right to:

- Know what personal information we collect, use, disclose, and (if applicable) sell or share
- Receive a copy of specific pieces of personal information we have collected
- Delete personal information, subject to legal exceptions
- Correct inaccurate personal information
- Limit the use and disclosure of sensitive personal information
- Opt out of the sale or sharing of personal information (we do not sell or share, but you have the right to make the request)
- Not receive discriminatory treatment for exercising your privacy rights

14.6 How to Exercise CCPA Rights

California residents may exercise their rights by contacting us as described in Section 19. We will verify your identity before responding and will respond within the timeframes required by the CCPA. You may use an authorized agent to make a request on your behalf, subject to verification.

14.7 Notice of Financial Incentive

We do not currently offer financial incentives in exchange for personal information.

14.8 California Shine the Light

Under California Civil Code Section 1798.83, California residents may request information about our disclosure of personal information to third parties for those parties' direct marketing purposes. We do not currently disclose personal information to third parties for their own direct marketing purposes.

15. Other U.S. State Privacy Laws

Residents of certain other U.S. states (including but not limited to Colorado, Connecticut, Virginia, Utah, Texas, Oregon, Montana, Delaware, Iowa, Tennessee, Indiana, New Jersey, and others as state laws come into effect) may have privacy rights under applicable state law, including:

- Right to access personal information
- Right to delete personal information

- Right to correct personal information
- Right to opt out of sale or targeted advertising
- Right to portability
- Right to limit processing of sensitive personal information
- Right to appeal denials of privacy requests

To exercise your rights under applicable state law, contact us as described in Section 19. We will respond within the timeframes required by your state's law.

16. Other Jurisdictions

If you are in a jurisdiction not specifically addressed above (such as Brazil under the LGPD, Canada under PIPEDA, Australia under the Privacy Act, Japan under the APPI, or other jurisdictions with applicable privacy laws), you may have additional rights under your local law. We honor rights that cannot be waived under applicable law and process personal information in accordance with the requirements of your jurisdiction. Contact us as described in Section 19 to exercise your rights.

17. Third-Party Services and Links

The Service may contain links to or integrate with third-party services, including Game developer applications, Payment Processor interfaces, app stores, and third-party websites. These third parties have their own privacy practices, which we do not control. We encourage you to review their privacy policies before providing personal information to them.

18. Changes to This Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, technology, legal requirements, or other factors. When we make material changes, we will update the Effective Date and provide notice through the Service or by other reasonable means before the changes take effect. Your continued use of the Service after the effective date of the updated policy constitutes acceptance of the updated terms, except where applicable law requires your express consent.

19. How to Contact Us

To contact us about this Privacy Policy or to exercise your privacy rights, please use the contact channels published in the INVO Policies. Current contact information for privacy inquiries, including our designated privacy contact, EU/UK representative (where applicable), and any additional channels required by your jurisdiction, will be published and updated through the Service.

We strive to respond to all privacy inquiries within the timeframes required by applicable law. If you are not satisfied with our response, you have the right to contact your local data

protection or privacy authority.

20. Payees: How to Exercise Your Rights

If you are a Payee, you can exercise the rights in Sections 12 to 16 by contacting us as described in Section 19. If you ask the Developer whose creator program you joined, it will forward your request to us. We may need to verify your identity before acting on your request. Some information must be kept for the periods in Section 7 even if you ask us to delete it.

--- END OF PRIVACY POLICY ---