

Privacy Policy

OnPoint Administration LLC

EFFECTIVE DATE: SEPTEMBER 11, 2026
LAST UPDATED: SEPTEMBER 11, 2026

OnPoint Administration LLC, a Delaware limited liability company ("**OnPoint**," "**we**," "**us**," or "**our**"), owns and operates OnPointCasino.com and its related websites, applications, and services (collectively, the "**Platform**"). We respect your privacy and are committed to protecting the personal information entrusted to us. This Privacy Policy (this "**Policy**") explains how we collect, use, disclose, retain, and protect your personal information when you access or use the Platform, and describes the choices and rights available to you.

By accessing or using the Platform, you acknowledge that you have read and understood this Policy and agree to the practices it describes. If you do not agree, please do not use the Platform. This Policy forms part of, and should be read together with, our Terms of Service and Sweepstakes Rules.

CONTENTS

01 Scope and About the Platform	09 Data Security
02 Information We Collect	10 Your Privacy Rights
03 How We Use Your Information	11 U.S. State Privacy Rights
04 Biometric Information	12 Eligibility and Children's Privacy
05 How We Share Your Information	13 Where We Process Your Information
06 Cookies and Tracking Technologies	14 Third-Party Links and Services
07 Communication Preferences	15 Changes to This Policy
08 Data Retention	16 Contact Us

01 SCOPE AND ABOUT THE PLATFORM

OnPointCasino.com is a social sweepstakes casino available to eligible adults located in permitted U.S. jurisdictions. The Platform uses two virtual currencies: **Gold Coins**, which are used for entertainment play only and have no monetary value; and **Sweeps Coins**, which cannot be purchased, are provided free of charge through promotions or an alternative method of entry, and may be redeemed for prizes in accordance with our Sweepstakes Rules. **No purchase is necessary** to participate in sweepstakes play. If this description conflicts with our Terms of Service or Sweepstakes Rules, those documents control.

This Policy applies to personal information we collect through the Platform, our customer support channels, our marketing communications, and any other interaction in which we link to this Policy. It does not apply to

third-party websites or services that we do not own or control. The Platform is intended solely for individuals located in the United States who meet our eligibility requirements.

02 INFORMATION WE COLLECT

2.1 Information You Provide to Us

- **Account registration:** full name, email address, date of birth, phone number, residential address, username, and password.
- **Identity verification (KYC):** government-issued photo identification, a selfie or live facial scan used for identity matching and liveness detection (see Section 4), proof of address, and, where required for enhanced due diligence, source-of-funds information.
- **Tax information:** Social Security Number or other taxpayer identification number, where required to satisfy tax reporting obligations associated with prize redemptions.
- **Payment and redemption information:** credit or debit card details (processed and tokenized by our third-party payment processors; we do not store full card numbers), bank account information for prize redemptions, and, where offered, digital currency wallet addresses.
- **Alternative method of entry (AMOE) requests:** the name, address, email address, and other details you include in a mail-in or other free entry request.
- **Responsible gaming settings:** self-exclusion requests, cool-off periods, purchase limits, and related preferences.
- **Communications:** messages you send to our support team or through the Platform, survey responses, feedback, and interactions with our official social media pages.

2.2 Information Collected Automatically

- **Device and browser information:** IP address, browser type, operating system, device identifiers, and similar technical data.
- **Usage and gameplay data:** pages visited, features used, time spent on the Platform, clickstream data, game activity, coin balances, and purchase and redemption history.
- **Geolocation data:** IP-based location and, with your permission, browser- or device-based location, used to verify jurisdictional eligibility and detect the use of VPNs, proxies, or other location-masking tools.
- **Cookies and similar technologies:** session and persistent cookies, pixels, tags, and software development kits (see Section 6).

2.3 Information We Receive from Third Parties

- **Identity verification providers (Sumsub):** identity verification results, document authenticity checks, liveness results, and sanctions, watchlist, and politically exposed person (PEP) screening results.
- **Payment processors and financial institutions:** transaction status, chargeback information, and fraud signals.
- **Fraud prevention and geolocation service providers:** risk scores, device reputation data, and location verification results.

- **Affiliate and referral partners:** referral codes, click identifiers, and campaign information showing how you arrived at the Platform.
- **Analytics providers:** aggregated usage statistics and performance measurements.

03 HOW WE USE YOUR INFORMATION

We use personal information for the following purposes:

- To create, maintain, and secure your account;
- To verify your identity, age, and eligibility, including your location in a permitted jurisdiction;
- To process Gold Coin purchases, administer sweepstakes, and process prize redemptions;
- To detect, investigate, and prevent fraud, money laundering, multiple or underage accounts, bonus abuse, and other prohibited activity;
- To comply with legal obligations, including anti-money laundering (AML), Bank Secrecy Act (BSA), sanctions (OFAC), and tax reporting requirements;
- To support responsible gaming, including enforcing self-exclusion and limit settings;
- To send transactional communications, such as account confirmations, security alerts, and redemption notices;
- To send promotional communications, with your consent where required by law;
- To measure the effectiveness of our marketing and to attribute referrals to our affiliate partners;
- To respond to customer support inquiries and resolve disputes;
- To analyze, maintain, and improve the Platform and develop new features; and
- To enforce our Terms of Service, Sweepstakes Rules, and other policies, and to protect the rights, property, and safety of OnPoint, our users, and others.

Automated tools. We use automated systems for identity verification, geolocation checks, and fraud detection. These systems may result in a verification failure or a temporary restriction on your account. If you believe an automated decision affecting your account is incorrect, contact us at support@onpointcasino.com and a member of our team will review it.

Legal Bases for Processing (Where Applicable)

- **Contract performance:** processing necessary to provide the services you request.
- **Legal obligation:** processing required by applicable law, including AML, tax, and sanctions compliance.
- **Legitimate interests:** fraud prevention, security, and Platform improvement.
- **Consent:** marketing communications, precise device geolocation, and biometric processing where required. You may withdraw consent at any time.

04 BIOMETRIC INFORMATION

As part of identity verification, our identity verification provider may capture a selfie or live facial image, compare it with the photo on your government-issued identification, and perform liveness detection. This process may involve creating a facial geometry template, which may be considered a biometric identifier or biometric information under applicable law ("**Biometric Data**").

- **Purpose.** We use Biometric Data solely to verify your identity, prevent fraud and duplicate or underage accounts, and comply with our legal obligations.
- **Notice and consent.** Before any Biometric Data is collected, we will inform you and obtain your consent, including written or electronic consent where required by applicable law (such as the Illinois Biometric Information Privacy Act).
- **No sale or profit.** We do not sell, lease, trade, or otherwise profit from Biometric Data.
- **Limited disclosure.** We disclose Biometric Data only to the identity verification provider acting on our behalf, with your consent, or as required by law or valid legal process.
- **Retention and destruction.** Biometric Data is permanently destroyed within a reasonable time after the purpose for its collection has been satisfied, and in any event no later than the earlier of (a) one year after that purpose expires or (b) three years after your last interaction with us, unless a longer period is required by law or valid legal process. Identity documents and verification results that are not Biometric Data are retained as described in Section 8.
- **Safeguards.** We protect Biometric Data using a reasonable standard of care that is at least as protective as the measures we use for our other confidential and sensitive information.

05 HOW WE SHARE YOUR INFORMATION

We do not sell your personal information for money. We may disclose personal information to the following categories of recipients:

- **Service providers:** payment processors, identity verification providers (Sumsub), fraud prevention and geolocation services, customer support and communications platforms, analytics providers, and cloud hosting providers. Service providers are contractually bound to use personal information only to perform services for us and to protect it appropriately.
- **Financial institutions:** banks, card networks, and payment partners involved in processing purchases, redemptions, and chargebacks.
- **Affiliate and marketing partners:** limited attribution information, such as a referral code or confirmation that a referred user registered or made a purchase. We do not share identity documents, Biometric Data, or payment details with affiliate partners.
- **Advertising and analytics partners:** online identifiers and activity data collected through cookies and similar technologies (see Sections 6 and 11).
- **Law enforcement, regulators, and legal process:** when required by law, subpoena, court order, or other government authority, including reporting obligations to the Financial Crimes Enforcement Network

(FinCEN), the Office of Foreign Assets Control (OFAC), and federal and state tax authorities, or when we believe disclosure is necessary to protect the rights, property, or safety of OnPoint, our users, or others.

- **Professional advisors:** attorneys, accountants, auditors, and insurers, subject to confidentiality obligations.
- **Business transfers:** in connection with an actual or proposed merger, acquisition, financing, reorganization, or sale of all or part of our assets, subject to confidentiality obligations.
- **With your consent or at your direction:** for any other purpose you authorize.

We may also share aggregated or de-identified information that cannot reasonably be used to identify you.

06 COOKIES AND TRACKING TECHNOLOGIES

We and our partners use cookies, pixels, tags, and similar technologies to operate the Platform, remember your preferences, analyze usage, measure marketing performance, and detect fraud.

TYPE	PURPOSE
Essential	Required for core Platform operation, such as logging in, maintaining your session, and processing transactions.
Security & Fraud Prevention	Help verify your device and location, protect your account, and detect prohibited activity.
Preference	Remember your settings and preferences.
Analytics	Help us understand how users interact with the Platform so we can improve it.
Advertising & Attribution	Measure the performance of our marketing campaigns and attribute sign-ups to affiliate and referral partners.

Your choices. You can block or delete cookies through your browser settings; disabling essential or security cookies may prevent parts of the Platform from working. You can also opt out of interest-based advertising through industry tools such as those offered by the Digital Advertising Alliance and the Network Advertising Initiative.

Global Privacy Control. We treat a Global Privacy Control (GPC) signal from your browser as a valid request to opt out of the sale or sharing of your personal information for that browser, where required by applicable law. Because there is no uniform industry standard for "Do Not Track" signals, we do not currently respond to them.

07 COMMUNICATION PREFERENCES

- **Transactional messages:** we will send account, security, and redemption-related messages as long as your account is active. These messages are not promotional and cannot be opted out of while you hold an account.
- **Email marketing:** you may unsubscribe at any time using the link in any promotional email or by contacting us.

- **Text messages:** if you consent to receive promotional text messages, you may opt out at any time by replying STOP. Consent to receive text messages is not a condition of any purchase. Message and data rates may apply.
- **Push notifications:** you may disable push notifications through your device settings.

08 DATA RETENTION

We retain personal information for as long as your account is active and thereafter for as long as necessary to fulfill the purposes described in this Policy, comply with our legal obligations, resolve disputes, and enforce our agreements. Specific retention periods include:

CATEGORY	RETENTION PERIOD
Account and transaction records	A minimum of five (5) years after account closure, consistent with Bank Secrecy Act recordkeeping requirements.
KYC and identity verification records	A minimum of five (5) years after account closure.
Biometric Data	As described in Section 4.
Tax records	As required by applicable federal and state tax laws.
Self-exclusion records	For the duration of the exclusion and thereafter as necessary to honor it.
Marketing preferences and communications	Until consent is withdrawn, plus two (2) years.
Customer support communications	Three (3) years.

When personal information is no longer required, we securely delete it or de-identify it so that it can no longer be associated with you.

09 DATA SECURITY

We implement administrative, technical, and physical safeguards designed to protect personal information, including TLS encryption for data in transit, encryption of sensitive data at rest, role-based access controls, authentication requirements, vendor due diligence, and regular security assessments. However, no method of transmission or storage is completely secure, and we cannot guarantee absolute security.

You are responsible for keeping your password confidential and for using multi-factor authentication where available. If you suspect unauthorized access to your account, contact us immediately at support@onpointcasino.com. If a security incident affects your personal information, we will notify you and the appropriate authorities as required by applicable law.

10 YOUR PRIVACY RIGHTS

Depending on where you live, you may have some or all of the following rights regarding your personal information:

- **Access:** request confirmation of whether we process your personal information and a copy of it.
- **Correction:** request that we correct inaccurate or incomplete information.
- **Deletion:** request deletion of your personal information, subject to legal retention obligations.
- **Portability:** request your information in a portable, machine-readable format.
- **Restriction:** request that we restrict processing of your information in certain circumstances.
- **Opt-out of marketing:** unsubscribe from promotional communications at any time.

How to submit a request. Email support@onpointcasino.com and describe your request. To protect your account, we will verify your identity before fulfilling a request, which may require you to log in or confirm information we already hold. Where permitted by law, you may use an authorized agent; we may require proof of the agent's authority and verify your identity directly.

Response timing. We aim to respond within 30 days, and in all cases within the time required by applicable law. If we need more time, we will notify you of the reason and the expected timeline.

Important: Some requests may be limited by our legal obligations. For example, we are required to retain certain account, transaction, and identity verification records under the Bank Secrecy Act and tax laws, even if you request deletion. Closing your account does not by itself delete these records.

11 U.S. STATE PRIVACY RIGHTS

11.1 California Residents (CCPA/CPRA)

This section supplements this Policy for California residents under the California Consumer Privacy Act, as amended by the California Privacy Rights Act (together, the "**CCPA**"). We collect, and in the preceding 12 months have collected, the following categories of personal information for the purposes described in Section 3:

CATEGORY	EXAMPLES	DISCLOSED FOR A BUSINESS PURPOSE TO
Identifiers	Name, email, phone number, postal address, username, IP address, device identifiers	Service providers; payment processors; identity verification providers; government authorities as required
Customer records	Date of birth, bank account information, identification details	Service providers; payment processors; identity verification providers; government authorities as required
Protected classification characteristics	Age and date of birth	Identity verification providers; service providers

CATEGORY	EXAMPLES	DISCLOSED FOR A BUSINESS PURPOSE TO
Commercial information	Gold Coin purchases, Sweeps Coin redemptions, gameplay and transaction history	Service providers; payment processors; affiliate partners (limited attribution data only); government authorities as required
Biometric information	Facial geometry derived from selfie or liveness checks	Identity verification provider only
Internet or network activity	Browsing and clickstream data, interactions with the Platform	Service providers; analytics and advertising partners; fraud prevention providers
Geolocation data	IP-based location and, with permission, device location	Geolocation and fraud prevention providers; service providers
Audio, electronic, or visual information	Selfie and ID images, support communications	Identity verification providers; customer support providers
Inferences	Fraud and risk assessments	Fraud prevention providers; service providers
Sensitive personal information	SSN, driver's license or passport number, account login credentials, financial account information, precise geolocation, biometric information	Identity verification providers; payment processors; tax authorities; service providers

Sale and sharing. We do not sell personal information for monetary consideration. However, our use of certain advertising and analytics technologies may be considered "sharing" of identifiers (such as cookie IDs and IP addresses) and internet or network activity for cross-context behavioral advertising under the CCPA. You may opt out of this sharing by enabling a Global Privacy Control signal or by emailing support@onpointcasino.com with "Do Not Sell or Share" in the subject line. We do not knowingly sell or share the personal information of consumers under 16 years of age.

Sensitive personal information. We use and disclose sensitive personal information only for purposes permitted under the CCPA regulations, such as providing our services, verifying identity, ensuring security and integrity, preventing fraud, and complying with law. We do not use it to infer characteristics about you.

Your California rights. Subject to certain exceptions, you have the right to:

- Know what personal information we collect, use, disclose, and share, and to access specific pieces of that information;
- Delete personal information we have collected from you;
- Correct inaccurate personal information;
- Opt out of the sale or sharing of personal information;
- Limit the use of sensitive personal information, to the extent it is used beyond the permitted purposes described above; and
- Not receive discriminatory treatment for exercising your privacy rights.

To submit a request, email support@onpointcasino.com with "California Privacy Request" in the subject line. Verification and authorized agent procedures are described in Section 10.

Shine the Light. We do not disclose personal information to third parties for their own direct marketing purposes.

11.2 Residents of Other States

Residents of states with comprehensive consumer privacy laws (such as Colorado, Connecticut, Oregon, Texas, and Virginia) may have the right, subject to applicable exceptions and thresholds, to:

- Confirm whether we process their personal information and access it;
- Correct inaccuracies in their personal information;
- Delete their personal information;
- Obtain a portable copy of their personal information;
- Opt out of targeted advertising, the sale of personal information, and profiling in furtherance of decisions that produce legal or similarly significant effects; and
- Provide or withdraw consent for the processing of sensitive data, where required.

To exercise these rights, email support@onpointcasino.com. **Appeals:** if we decline to take action on your request, you may appeal by emailing us with "Privacy Request Appeal" in the subject line. We will respond to your appeal within the time required by applicable law. If your appeal is denied, you may contact your state Attorney General.

11.3 Nevada Residents

Nevada residents may submit a request directing us not to sell their covered information. We do not sell covered information as defined under Nevada law, but you may submit a request to support@onpointcasino.com.

12 ELIGIBILITY AND CHILDREN'S PRIVACY

The Platform is intended only for individuals who are at least 18 years of age, or the age of majority in their jurisdiction if higher, and who meet the other eligibility requirements in our Terms of Service. The Platform is not directed to children, and we do not knowingly collect personal information from anyone under 18. If we learn that we have collected personal information from a person under 18, we will close the account and promptly delete that information, except where retention is required by law. If you believe a minor has provided us with personal information, contact us at support@onpointcasino.com.

13 WHERE WE PROCESS YOUR INFORMATION

The Platform is intended for users located in the United States, and we store and process personal information primarily in the United States. Some of our service providers, including identity verification providers, may process personal information in other countries. When they do, we require appropriate contractual and technical safeguards to protect your information.

14 THIRD-PARTY LINKS AND SERVICES

The Platform may contain links to third-party websites, social media platforms, or services. We are not responsible for the privacy practices of those third parties, and we encourage you to review their privacy policies before providing any personal information.

15 CHANGES TO THIS POLICY

We may update this Policy from time to time to reflect changes in our practices, technologies, or legal requirements. Material changes will be communicated by email or by a prominent notice on the Platform before they take effect. The "Last Updated" date at the top of this Policy reflects the most recent revision. Your continued use of the Platform after an updated Policy takes effect constitutes your acknowledgment of the updated Policy.

16 CONTACT US

For privacy-related questions, requests, or concerns, please contact our Privacy Team. To help us route your message, please use the subject lines below where applicable.

REQUEST TYPE	SUBJECT LINE
General privacy questions or rights requests	Privacy Request
California residents	California Privacy Request
Opt out of sale or sharing	Do Not Sell or Share
Appeal of a denied request	Privacy Request Appeal

ONPOINT ADMINISTRATION LLC — PRIVACY TEAM

Email: support@onpointcasino.com

Website: OnPointCasino.com