LEGAL

Privacy Policy

Last updated: November 4, 2026

Changes effective: November 10, 2026

This policy explains what personal data PollsLive collects, why we collect it, how we protect it, and the rights you have over it. We aim to collect as little as possible and to be clear about the rest.

---

1. Data Controller

PollsLive is operated by **A Plus Apps**, registered with the Dutch Chamber of Commerce (KVK) under number **42117052** and established in the Netherlands ("we", "us", "our"). We are the data controller for the personal data described in this policy, except where section 2 says otherwise. Our lead supervisory authority is the Dutch Data Protection Authority (**Autoriteit Persoonsgegevens**). We are not required to appoint a Data Protection Officer under Article 37 GDPR and have not appointed one; privacy matters are handled directly by the team at support@pollslive.com or through our contact form.

2. Controller & Processor Roles

For your **account** (your name, email, workspace, billing status and support history), we are the **controller**: we decide why and how that data is processed, and this policy governs it.

For the **content and responses inside a workspace** (the questions a creator writes, the votes and open-text answers participants submit, and any lead-capture fields a creator switches on), the workspace owner is the controller and we act as a **processor** on their instructions. If you answered a poll and want your response removed, contact the organisation that ran it; we will help them action it, and will act ourselves where the law requires.

Our Data Processing Agreement under Article 28 GDPR sets out that processing in full and applies to every workspace automatically. You do not have to request it. It incorporates the EU Standard Contractual Clauses where they are needed for onward transfers. If your procurement team needs a countersigned copy, email support@pollslive.com.

Your obligations when you are the controller. If you run polls or live sessions, you must have a lawful basis for any personal data you collect from participants, provide any privacy notice the law requires, and obtain consent where it is required. We process that data on your instructions under the DPA; we do not check whether your notice or consent is adequate. See also the Your Content section of our Terms.

If you answer a poll or join a live session. The person or organisation running it decides what to ask and what happens to your answers: they are the controller and should tell you how they use them, and we run the Service for them as processor. We are the controller only for what keeps voting fair and the Service secure: a random browser token in the **pollslive_voter** cookie (12 months) and security and abuse logs (12 months). You do not need an account, and you can answer without giving your name. Your answers are kept until the organiser deletes them or closes their workspace. To see, correct or delete your answers, contact the organiser; you can also contact us and we will pass your request on, or act ourselves where the law requires. You can complain to your data protection authority; ours is the Dutch Autoriteit Persoonsgegevens.

3. Data We Collect

Account data: name, email address, password hash (for credential sign-in) or Google account identifier (for OAuth sign-in), workspace membership, and billing status. For paid accounts we also store what our payment provider returns about a charge: the billing country, city and state, the card brand and last four digits, the payment method type, and the provider's fraud score for that payment. We never receive or store the full card number.

Poll content: questions, options, themes, slide decks, and published poll configurations you create.

Vote & participation data: selected options, nicknames you choose in live sessions, and timestamps. We use a protected browser token and server-side abuse prevention to limit duplicate voting without requiring an account. Vote records do not contain a voter's name, email, or raw IP address unless the participant voluntarily supplies a display name. That makes votes pseudonymous rather than anonymous in the legal sense: answers from the same browser can be linked to each other, but not to a name unless the participant gives one.

Contact submissions: when you use our contact form, we store your name, email, selected category, subject, message, and any files you attach, together with a hashed IP address and browser user agent for abuse prevention. Our database keeps only the hash; the notification email we send to our own support mailbox also carries the raw address, so a human can act on a malicious submission. That email is delivered by the provider named under Sub-processors. We use this solely to handle your request.

Lead capture (optional): if lead capture is on for a poll or survey, we store the contact fields a respondent fills in (for example email, name or company), only when they tick the consent box, and the delivery status to your destinations. On plans that include it, lead capture is on by default for the event feedback survey sent after a live session.

PollsLive news: if you ask for PollsLive product news, in the site footer or with the optional box on an event feedback survey, we store your email address, where you signed up and a hashed IP

address. The box is never ticked for you, we send nothing but a confirmation email until you confirm the address, and you can withdraw your consent at any time. The organizer of the survey does not see this choice.

Pulse AI chat: when you use the Studio assistant, we store conversation transcripts needed to continue the chat and improve support quality.

Content sent to AI features: when you use Pulse AI to draft or branch a poll, your prompts and the poll content go to our AI processor, which routes them only to model providers that do not store prompts or use them for training. If a host runs an AI response digest on a poll, the **participants' open-text answers for that poll** go only to a provider whose terms forbid keeping them or using them for training; when none is configured, our rule-based engine writes the digest instead. Providers are named on our Sub-processors page.

Referral source: if you arrive from a link that names where it came from (for example a software directory or our newsletter), we store that single short label (such as "g2" or "newsletter") against your workspace, once, when the workspace is created. It records which channel introduced you to PollsLive so we know which ones are worth our effort. It is never overwritten, it is not linked to any advertising network, and we set no cookie and store nothing on your device to collect it.

Usage & technical data: pages visited, feature usage, outbound mail delivery logs, and security logs used to operate, secure, and improve the Service.

4. How We Use Data

- Provide, maintain, and improve the polling Service
- Authenticate creators and manage workspaces
- Process subscriptions and prevent payment fraud
- Display real-time and aggregated poll results
- Respond to support, billing, and privacy requests
- Detect, prevent, and investigate abuse and security incidents

5. Legal Bases (GDPR)

Where the GDPR applies, we rely on these legal bases. **Performance of a contract:** providing the Service to account holders, taking payment, the AI features you ask for, and account and billing email. **Legitimate interests:** securing the Service, preventing duplicate votes, vote manipulation and abuse, payment-fraud checks, answering enquiries, recording which link brought you to us, and understanding aggregate product usage, balanced against your rights each time. **Legal obligation:** tax and accounting records and responding to lawful requests. **Consent:** non-

essential analytics and the Whop Pixel, and PollsLive news by email. Lead-capture details and poll answers are processed for the host who runs the poll, who decides the legal basis for them. To create an account you must give us an email address and a password or Google sign-in, and to buy a plan you must give Whop your payment details; without them we cannot provide those parts of the Service. Participants do not have to give us any personal data to answer a poll. Where we rely on consent you may withdraw it at any time, and withdrawal is as easy as giving it. Where we rely on legitimate interests you have the right to object.

6. Automated Decisions & Profiling

We do not carry out automated decision-making that produces legal or similarly significant effects about you within the meaning of Article 22 GDPR, and we do not build marketing or behavioural profiles for advertising. Three automated processes do run. Anti-abuse checks score a request (rate limits, bot challenges, duplicate-vote detection) to keep polls fair. Our payment provider returns a fraud score attached to each payment, which we store and may consider when investigating a disputed or suspicious charge; it never decides on its own whether you may use the Service. The optional Pulse AI features generate suggested poll content at your request, and a human is always the one who publishes. If any of these blocks you in error, contact us and a person will review it: you can ask for human review, express your view, and contest the outcome.

7. Sub-processors

We use a small number of trusted sub-processors to deliver the Service. The table below lists those that handle the most common personal-data flows.

Sub-processor	Service type	Location / jurisdiction	Data transferred
Whop Inc.	Payment processing and billing (Merchant of Record)	United States / global (EU Standard Contractual Clauses)	Billing details, em transaction reco
Hostinger	Cloud infrastructure and compute	European Union data centres	Database record application logs
MXroute	Transactional email and auth mail	United States / global (EU Standard Contractual Clauses)	Account email, m links, billing notic

A full, current sub-processor schedule with every provider we use is on our Sub-processors page.

8. Third Parties

- **Whop**: payment processing and subscription management, acting as Merchant of Record
- **Google**: optional single sign-on (OAuth) for account access
- **Cloudflare**: DNS, CDN and bot protection (Turnstile)
- **OpenRouter**: our AI provider for Pulse AI chat and generation; it forwards each request to the provider of the selected model. We route requests only to model providers that do not store prompts or use them for training, and we do not use free model tiers.
- **MXroute**: transactional email delivery (account, billing, and product mail)
- **Hostinger**: EU-based hosting for our application, database, and cache

A full, current list with each provider's purpose, the data it handles, and its location is on our Sub-processors page. We do not sell personal data to third parties.

9. Cookies & Local Storage

We set a small number of strictly necessary cookies: a sign-in session cookie, CSRF and sign-in-flow tokens, a signed **pollslive_voter** cookie that prevents duplicate voting without forcing a login, a per-poll access cookie set only when you enter a PIN for a protected poll, and a **NEXT_LOCALE** cookie that remembers which language to serve you. We use browser local storage for your consent choice, a client-side "already voted" flag, and live-session nicknames. Changes to a deck you are editing that have not been saved yet are also kept there until they are saved. Non-essential analytics and attribution (Cloudflare Web Analytics and the Whop Pixel, which tells Whop, our merchant of record, which page or campaign led to a purchase) load only after you accept them in the consent banner. Cloudflare Zaraz is not enabled on PollsLive. Our CDN and payment provider may set their own strictly necessary cookies. Full detail, including lifetimes, is in our Cookie Policy.

10. Data Security

Traffic is encrypted in transit. Credentials are protected using industry-standard one-way storage, and access to production systems is restricted. We use appropriate technical and organisational measures to protect personal data and review those measures as the service changes.

11. Data Breaches

We maintain procedures to detect, investigate and record personal data breaches. Where a breach is likely to result in a risk to your rights and freedoms, we will notify the Autoriteit

Persoonsgegevens without undue delay and, where feasible, within 72 hours of becoming aware of it, as required by Article 33 GDPR. Where the risk is high, we will also inform affected users directly and without undue delay under Article 34. Where we act as a processor for a workspace owner, we will notify that customer without undue delay so they can meet their own obligations.

12. International Transfers

Our core application infrastructure is hosted in Germany, inside the EU. Some processors are based in, or may process data in, countries outside the EEA, including the United States: Whop, Google, Cloudflare, MXroute, Slack (only if you connect it) and OpenRouter, with the AI model providers it routes to. For each such transfer we rely on the EU-US Data Privacy Framework where the recipient is certified under it, and otherwise on the European Commission's Standard Contractual Clauses (with the UK Addendum for UK data), with supplementary measures where needed. You can ask us for a copy of the relevant safeguards.

13. Retention & Deletion

We keep personal data only as long as we need it. A scheduled job enforces the time limits below for security, abuse and audit logs, outbound mail delivery logs, stored copies of email bodies, password-reset records, Pulse AI conversations and expired IP bans. **Account data** is kept while your account is active and removed when you delete it; **poll content and responses**, including **lead-capture details**, until the host deletes them or the workspace is closed; **security, abuse and audit logs** and **outbound mail delivery logs** for 12 months; **stored copies of email bodies** for 90 days; **Pulse AI assistant conversations** for 180 days after the last message; **PollsLive news sign-ups** until you unsubscribe; **contact-form submissions and attachments** until your request is resolved and any related obligation has passed (we review and delete these by hand rather than on a fixed day count, because a sales or legal thread can outlive a generic purge window); **password-reset records** for 12 months. Expired IP bans are lifted automatically and then deleted, as are bans we lift by hand; a ban still in force is kept until we lift it.

What we keep after you delete your account. Billing and invoice records, including refunds and the email address attached to them, are kept for 7 years because Dutch tax law requires it. Article 17(3)(b) GDPR allows us to retain data where a legal obligation applies. We also keep a deletion record: the time, whether you or an admin deleted the account, the plan, the language, and counts of workspaces, polls and sessions, plus a keyed hash of the email address so a later sign-up of the same address can be recognised. That record does not include your name or the address itself. Feedback answers are deleted with the account. Everything else tied to your account, including your mail delivery logs, is deleted with it.

The deletion record also holds the account's internal id, the date the account was created, how you told us you found PollsLive, and the reason you picked when deleting, if any. It is deleted 3 years after the account. IP bans we lift by hand are deleted 12 months after they are lifted. An address that bounced or unsubscribed stays on our do-not-email list for 12 months, so we do not mail it again.

Deletion is immediate in the application and propagates to backups within 35 days, after which backup copies are rotated out.

14. Your Rights

Depending on your jurisdiction (including under the GDPR and the UK GDPR), you may have the right to access, correct, delete, restrict or port your personal data, to object to processing based on legitimate interests, and to withdraw consent at any time. Most of these you can exercise yourself from Studio → Account & privacy; for anything else, contact us and we will respond within one month, as Article 12(3) requires. We do not charge for these requests and will not treat you worse for making one. If you are unhappy with our response you have the right to complain to your local supervisory authority: for us that is the Dutch **Autoriteit Persoonsgegevens** (autoriteitpersoonsgegevens.nl), and in the UK the **Information Commissioner's Office** (ico.org.uk). Participants and former users can also use our privacy request form.

15. US State Privacy Rights

If you are a resident of California (CCPA/CPRA) or another US state with a comprehensive privacy law (such as Virginia, Colorado, Connecticut, or Utah), you have the right to know what personal information we collect, to access and delete it, to correct inaccuracies, and to opt out of the "sale" or "sharing" of personal information and of targeted advertising.

We do not sell your personal information, we do not use it for cross-context behavioural advertising, and we have not done so in the preceding twelve months. One consented script, the Whop Pixel, reports page views and purchase attribution to Whop, our merchant of record; to the extent that counts as "sharing" under your state's law, rejecting analytics in the consent banner, or in Studio → Account & privacy, is your opt-out and keeps the pixel off. We do not knowingly collect or process sensitive personal information for the purpose of inferring characteristics. You may exercise your access, deletion, correction and portability rights from Studio → Account & privacy or by contacting us, and you will not be discriminated against for doing so. You may use an authorised agent where your state allows it.

Global Privacy Control. If your browser sends a Global Privacy Control (GPC) signal, we treat it as your opt-out of sale and sharing: analytics and the Whop Pixel stay off and the consent banner does not ask. You can change this under **Your privacy choices** at the foot of every page.

Appeals. If we decline a privacy request, we will tell you why. Residents of states that provide an appeal right (including Virginia, Colorado, Connecticut, Montana, Texas and Oregon) may appeal that decision by replying to our response or emailing support@pollslive.com with "Privacy appeal" in the subject. We will review and respond within 45 days. If we deny the appeal, you may contact your state Attorney General.

16. Children's Privacy & Schools

PollsLive is not directed at children. By creating an account you confirm you are at least 16, or 13 where local law allows a lower age with appropriate consent. We do not ask for a date of birth at sign-up, and we do not knowingly collect personal data from children below that age. If you believe a child has provided us personal data, contact us and we will delete it promptly.

Classroom use. Teachers and institutions do use PollsLive with students. Where that happens, the school or institution is the controller for the classroom activity and is responsible for having the appropriate legal basis or parental consent under the GDPR (Article 8), the US Children's Online Privacy Protection Act (COPPA) and any local schools legislation. Students answer polls without an account and without being asked for a name unless the teacher enables nicknames, which keeps the personal data involved to a minimum by design.

Learning management systems. PollsLive does not receive class rosters or student records from a learning management system (LMS): a launch from an LMS opens the poll, and the student joins like any other participant.

17. India & Other Regions

If you are in India, we handle your personal data in line with the Digital Personal Data Protection Act, 2023 (DPDP Act) and its Rules. You have the right to access, correct, and erase your personal data, the right to grievance redressal, and the right to nominate another person to exercise your rights on your behalf. To raise a grievance, contact support@pollslive.com with "DPDP grievance" in the subject and we will respond within the timelines required by law; if you are not satisfied with our response, you may escalate to the Data Protection Board of India. In all other regions, we apply the safeguards described in this policy (GDPR-level protections) to everyone who uses the Service, wherever you are.

18. Changes

We may update this policy, for example when we add a feature, change a processor, or when the law changes. The current version is always on this page with its effective date. For changes that materially affect your rights or how we use your data, we will give at least **30 days' notice** before

they take effect, by a notice on the Service and by email to account holders where we hold a verified address. Where a change requires your consent under applicable law, we will ask for it rather than assume it. Continued use after a non-material change takes effect constitutes acceptance; if you do not accept a material change, you may delete your account before it takes effect.

19. Contact

Privacy requests: support@pollslive.com, or use our contact form and choose "Privacy / GDPR".