LEGAL

Data Processing Agreement

Last updated: November 5, 2026

Changes effective: November 30, 2026

This is the data processing agreement required by Article 28(3) GDPR for customers who run polls, surveys or live sessions with PollsLive. It applies automatically to every paid and free workspace (you do not have to request it) and forms part of our Terms and Conditions. A countersigned copy is available for procurement files.

---

1. Parties and scope

This agreement is between you (the workspace owner, referred to here as the **customer**) and **A Plus Apps**, registered with the Dutch Chamber of Commerce (KVK) under number **42117052** and established in the Netherlands, operating the PollsLive service. It governs our processing of personal data on your behalf and takes precedence over anything to the contrary in the Terms and Conditions on that subject. Nothing in it reduces a right you hold under the GDPR.

2. Who is controller, who is processor

For the **content and responses inside your workspace** (the questions you write, the votes and open-text answers your participants submit, the nicknames they choose, and any lead-capture fields you switch on), **you are the controller and we are the processor**. You decide what to ask, who to ask, and how long to keep it. This agreement covers that processing.

For **your own account** (your name, email, workspace, billing status and support history), **we are the controller**, and our Privacy Policy governs it rather than this agreement. The split is the same one set out in section 2 of that policy.

Where a school, employer or other institution runs sessions with PollsLive, that institution is the controller for the classroom or workplace activity and this agreement runs to it.

3. Subject matter, duration, nature and purpose

Subject matter and purpose. Providing the PollsLive service: hosting polls, surveys and live sessions, collecting and counting responses in real time, presenting results, and producing exports and summaries at your request.

Nature of processing. Collection, recording, storage, structuring, retrieval, display, export, and erasure, by automated means. Where you use our AI features, this also includes transmission to the AI processor named on our Sub-processors page. Note that running an AI response digest sends your participants' open-text answers for that poll.

Duration. For as long as your workspace exists, and thereafter only for the period described in section 10.

Categories of data subject. Your participants and respondents, the members you invite to your workspace, and any people identified in the content you upload.

Types of personal data. Responses to your questions, including free-text answers; nicknames or display names participants enter; any contact or lead-capture fields you choose to collect; workspace member names and email addresses; and technical data used to prevent duplicate voting, which is a one-way pseudonymous value and not a stored address. We do not ask you for special-category data under Article 9, and the service is not designed to hold it. If your questions elicit it, you remain the controller for that decision.

4. Processing on documented instructions

We process personal data only on your documented instructions, including as to international transfers. Your use of the service (the polls you create, the settings you choose, the exports you run) constitutes those instructions, together with this agreement and the Terms. If EU or member-state law requires us to process on some other basis, we will tell you before doing so unless that law forbids the notification. If we believe an instruction infringes data protection law, we will tell you.

5. Confidentiality

Access to production systems is limited to the people who need it to operate and support the service, and they are bound by confidentiality obligations that survive the end of their engagement. We do not read workspace content except where it is necessary to provide support you have asked for, to investigate an abuse report, or where the law requires it.

6. Security measures (Article 32)

The technical and organisational measures in place today. They are described in more depth on our Security page; this list is what we are contractually committing to, and we may change a specific measure provided the overall level of protection is not reduced.

- **Encryption in transit.** All traffic is served over TLS, terminated at our CDN, with HTTP Strict Transport Security enforced.
- **Credential storage.** Passwords are protected using industry-standard one-way storage. We never hold a recoverable copy.
- **Data minimisation for anti-abuse.** Technical identifiers used to prevent abuse are minimised, protected, and retained only as needed for the relevant security purpose.
- **Infrastructure security.** Service data is hosted in the European Union with layered network and access controls.
- **Access control.** Workspace access is role-based, administrative actions are audited, and production access is limited to authorised personnel.
- **Application hardening.** We use browser security controls, request limits, automated abuse prevention, and security monitoring appropriate to the service.
- **Upload safety.** Images are re-encoded on ingest, which strips embedded metadata and anything that is not image data, and unsafe file types are refused.
- **Resilience.** Backups run on a schedule, are kept off-site, and are restore-tested rather than assumed. Retention limits are enforced by a scheduled job rather than left aspirational.
- **Availability of your data to you.** Workspace owners can export their data and erase their account without asking us, so neither depends on our response time.
- **Patching and vulnerability management.** Operating-system security updates are applied automatically, and host configuration is audited regularly. Application dependencies are monitored for published vulnerabilities and updated on a rolling basis.
- **Stored data.** Access to stored service data is restricted and sensitive credentials use one-way protection.

7. Sub-processors

You give general authorisation for us to engage sub-processors. The current list, with each one's purpose, the data it handles and where it is located, is published and kept current at Sub-processors. That page is the schedule to this agreement rather than a copy of it, so the two cannot drift apart.

Each sub-processor is bound by a written agreement imposing data protection obligations no less protective than those in this agreement, and we are liable to you for their performance as for our own, within the limits of liability in section 20 of our Terms and Conditions. When we plan to add or replace a sub-processor, we update that page with the change and the date it takes effect at least 30 days before it starts processing your data, unless we must act sooner to keep the Service secure or available, in which case we update it as soon as we can. Any customer can ask

through our contact form to be told of such changes directly, and can object on reasonable data protection grounds before the change takes effect. If we cannot address the objection, you may end the affected service and we refund any prepaid fees for the unused period.

8. Assisting with data subject rights

Taking account of the nature of the processing, we assist you by appropriate technical and organisational measures in meeting requests from your participants to access, correct, erase, restrict, port or object to processing of their data. In practice most of this is self-serve: workspace owners can view, export and delete responses directly. If a participant contacts us about a poll you ran, we will refer them to you as the controller and help you action the request. Where a request reaches us and the law requires us to act ourselves, we will.

9. Breach notification and assessments

We maintain procedures to detect, investigate and record personal data breaches. Where a breach affects personal data we process for you, we will notify you **without undue delay, and in any event within 48 hours** after becoming aware of it, with the information you need to meet your own Article 33 obligation: what happened, the categories and approximate number of records concerned, the likely consequences, and the measures taken. Where we do not yet have all of that, we send what we have and follow up. Notifying your supervisory authority remains your decision as controller.

We assist you, taking account of the nature of processing and the information available to us, with data protection impact assessments and prior consultation under Articles 35 and 36.

10. Return and deletion

At any time during the service you can export your workspace data in a machine-readable form, so return does not depend on termination.

When you delete your account or close your workspace, we delete the personal data we process for you, except where EU or member-state law requires us to keep it, notably billing records, which are subject to a Dutch retention obligation and are disclosed in our Privacy Policy rather than deleted. We delete it from our live systems within 30 days, and it leaves our backups as they rotate out, within a further 35 days. On request we confirm the deletion in writing.

11. Information and audit

We make available to you the information necessary to demonstrate compliance with Article 28, and allow for and contribute to audits, including inspections, conducted by you or an auditor you mandate.

In the first instance we will answer a written security questionnaire and provide a written overview of our controls, data residency and review practices, which for most customers settles the question without an on-site visit. Where that is genuinely not sufficient, an audit may be carried out on reasonable notice, no more than once a year unless a breach or a supervisory authority requires otherwise, during business hours, subject to confidentiality, and in a way that does not disrupt the service for other customers. We are a small company: we do not publish detailed audit reports on the public internet, and we say so rather than implying a certification we do not hold.

12. International transfers

Our core application and database are hosted in the European Union. Where a sub-processor may process personal data outside the EEA, that transfer is made under an appropriate Article 46 safeguard: in practice the European Commission's Standard Contractual Clauses, and where relevant the EU-US Data Privacy Framework. The Module Two (controller-to-processor) clauses are incorporated into this agreement by reference for any such transfer, with this agreement's Annexes supplied by sections 3, 6 and 7 above.

13. Getting a signed copy

This agreement is already in force for your workspace; no signature is needed for it to apply. If your procurement or legal team needs a countersigned PDF, or needs it executed on your own paper, email support@pollslive.com or use our contact form and choose "Privacy / GDPR". Questions about anything above go to the same place.