

Data Processing Agreement

Version 1.2 · October 2026

This Data Processing Agreement (“DPA”) sets out the terms under which **suPlay B.V.** (“Processor”) processes Personal Data on behalf of the Customer (“Controller”) in connection with the suPlay Poll service. It is designed to meet the requirements of Article 28 of the General Data Protection Regulation (Regulation (EU) 2016/679, “GDPR”).

This DPA is in force for every account — no signature is required. It is incorporated by reference into the [Terms of Service](#) (§13), which govern every account, and Art. 28(9) GDPR requires this contract to be in writing “including in electronic form”. That applies on every plan, free tiers included, whenever you use the Services to process Participant personal data as a Controller. The signed copy below is offered because some procurement processes require one — it does not create the agreement, and declining to sign does not remove it.

If you need a signed copy, either route works and both take up to five business days:

- Download the [PDF version](#), complete and sign Annex A, and email it to privacy@suplay.nl — we counter-sign and return it.
- Or email privacy@suplay.nl with your legal name, registered address and signing contact, and we will send a pre-filled copy for signature. Enterprise-tier customers can sign via DocuSign on request.

1. Definitions

- **“Personal Data”, “Processing”, “Controller”, “Processor”, “Subprocessor”, “Data Subject”** have the meanings given in the GDPR.
- **“Services”** means the suPlay Poll service as described in our [Terms of Service](#).
- **“Main Agreement”** means the contractual terms under which the Controller uses the Services (our Terms of Service plus any signed order form).

2. Subject matter and duration

This DPA applies to all Processing of Personal Data carried out by suPlay B.V. on behalf of the Controller under the Main Agreement. It is in force for the duration of the Main Agreement and survives until all Personal Data processed hereunder has been deleted in accordance with §10.

3. Nature and purpose of processing

The Processor processes Personal Data solely to provide the Services: to operate presenter accounts, run live polls, deliver transactional email, handle billing, and maintain the Services. A description of the Processing activities, categories of Data Subjects, and categories of Personal Data is set out in **Annex B**.

4. Documented instructions

The Processor processes Personal Data only on documented instructions from the Controller, including regarding transfers to a third country. The Main Agreement, this DPA, and the use of the Services through their user interfaces and APIs constitute such documented instructions. The Processor

will inform the Controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data-protection provisions.

5. Confidentiality of personnel

The Processor ensures that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

6. Security (Art. 32)

The Processor implements appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including those described on our [Security Summary](#) page. The measures include, at minimum:

- TLS 1.2+ for all external traffic; HSTS enforced.
- Encryption of backups at rest.
- bcrypt password hashing (cost 12) and SHA-256 token hashing.
- Rate limiting on authentication, signup, and email-resend endpoints.
- Application runs as an unprivileged system user.
- Quarterly security-incident tabletop exercises and monthly restore tests.
- Error-monitoring PII scrubbing (`sendDefaultPii: false`).
- Audit logging of administrative impersonation.

7. Subprocessors

The Controller gives the Processor **general written authorisation** to engage Subprocessors under Art. 28(2) GDPR, and authorises those listed on our [Subprocessors](#) page as of the Effective Date. The Processor will:

- Impose contractual obligations on each Subprocessor that are no less protective than this DPA (Art. 28(4)).
- **Publish the full candidate list in advance.** The Subprocessors page names every Subprocessor the Platform is able to engage, including every AI provider, with its role, data categories, region, transfer basis, and whether an Art. 28(3) data-processing agreement and, for processing outside the EEA, Standard Contractual Clauses are in force. **A Subprocessor may only be engaged once those are in force and the page says so.**
- **Bringing a listed Subprocessor into service is within this authorisation** and is not the addition of a Subprocessor, because it was disclosed and contractually covered in advance. That includes the Platform's automatic failover to it. Engaging a Subprocessor that is *not* already listed is an addition and is notified as below.
- Give the Controller at least **14 days'** notice, by email to the contact the Controller nominates, before adding a Subprocessor that is not already listed. **Where a change is required for security, service continuity, or compliance with a legal obligation**, the Processor may make it on shorter notice or with immediate effect, informing the Controller without undue delay; the objection and termination rights below are unaffected.
- Allow the Controller to object on reasonable grounds within 14 days of that notice (or, for an urgent change, of being informed). The parties will seek a resolution in good faith; failing that, the Controller may terminate the affected subscription on a pro-rata basis.

A Controller may subscribe to these notifications by emailing privacy@suplay.nl.

8. Assistance (Arts. 28(3)(e), (f))

Taking into account the nature of the Processing, the Processor assists the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to

requests for exercising Data Subject rights (Chapter III GDPR), data breach notification, data protection impact assessments, and prior consultation with the supervisory authority.

- Presenter accounts: self-service via the **/settings** page and documented endpoints.
- Participant data: on request via privacy@suplay.nl within 30 days.

9. Personal-data breach notification (Art. 33)

The Processor notifies the Controller without undue delay, and in any case **within 72 hours** of becoming aware, of any Personal Data breach affecting the Controller's data. The notification describes the nature of the breach, categories and approximate number of affected Data Subjects, likely consequences, and remediation measures taken or proposed.

10. Return or deletion of Personal Data

On termination of the Main Agreement, the Controller may export its Personal Data for **30 days**. After that period, the Processor deletes all Personal Data processed under this DPA from live systems within **90 days**. Copies inside encrypted database backups expire on the backup rotation schedule: daily backups within 30 days, monthly backups within **12 months**. Until then those copies remain encrypted at rest, are not used for any processing other than disaster recovery, and any Personal Data reintroduced by a restore is deleted again without undue delay. The foregoing applies unless Union or Member State law requires longer storage (for example, Dutch tax law requires billing records to be retained for seven years).

11. Audit (Art. 28(3)(h))

The Processor makes available to the Controller all information necessary to demonstrate compliance with Art. 28 GDPR, including this DPA, the Subprocessors page, the Security Summary, and our internal processing inventory on request. Where the Controller reasonably requires further evidence, the Processor will support remote, questionnaire-based audits at no cost, and on-site audits at the Controller's reasonable expense. The Controller will provide at least 30 days' notice and will not disrupt operations.

12. International transfers

Where Personal Data is transferred outside the European Economic Area to a Subprocessor, the transfer is made on the basis of the European Commission's Standard Contractual Clauses (Decision 2021/914 or any successor), unless the recipient country has an adequacy decision under Art. 45 GDPR.

13. Liability and order of precedence

Each party's liability under this DPA is subject to the liability limits of the Main Agreement. In case of conflict between this DPA, the Main Agreement, and the GDPR, the GDPR prevails, then this DPA, then the Main Agreement.

14. Governing law and jurisdiction

This DPA is governed by the laws of the Netherlands. Disputes are subject to the exclusive jurisdiction of the courts in Overijssel, the Netherlands, without prejudice to a Data Subject's statutory rights of complaint to a supervisory authority.

Annex A — Parties (to be completed by the Customer)

Processor: suPlay B.V., Ruwerstraat 9, 7545 SM Enschede, The Netherlands. KvK: 70176264. VAT: NL858175691B01. Represented for signature by Holger Schiele, Managing Director. Data Protection contact: Frederik Vos (Co-founder, Head of Development), privacy@suplay.nl.

Controller:

- Legal name: _____
- Registered address: _____
- Company registration (KvK / trade register / equivalent): _____
- VAT ID: _____
- Represented by (name, title): _____
- Privacy contact (name, email): _____
- Effective date: _____

Signatures. The instructions above ask the Controller to sign and the Processor to counter-sign, so both blocks belong here.

- For the Controller — name: _____ · title: _____
_____ · signature: _____ · date: _____
- For suPlay B.V. — name: _____ · title: _____
_____ · signature: _____ · date: _____

Annex B — Processing description

Subject matter and duration: operation of the suPlay Poll service, for the duration of the Main Agreement.

Nature and purpose: delivering a live-polling platform for presenters and their audiences, with associated transactional email, billing, error monitoring, and AI-assisted features that form part of the Services.

AI-assisted processing: automated moderation of participant free text, which runs on submissions as part of delivering the Services; and summaries of open-text answers, question suggestions and translation drafts, which a presenter initiates. Availability of these features is operated by the Processor at platform level; the Controller's instruction for them is constituted by use of the Services under §4. The Controller may withdraw that instruction at any time: when AI processing is switched off for an account (in its settings) or for a team organization (by its owner or an administrator), no content of the events that account owns or that organization holds, and nothing that account submits to an AI feature, is sent to any language model, the Processor's own or a Subprocessor's, from the next request on. Participant free text is then not screened by a language model: text that the Platform's built-in word list marks as high-risk is held for the presenter's approval, and other text follows the event's own approval settings. Content is processed on our self-hosted model on EU infrastructure; where that model cannot serve a request it may be processed by a provider listed on our [Subprocessors](#) page. Our configuration requires such a provider to be EEA-resident, so processing stays inside the EEA unless a transfer is made on the basis set out in §12. On either path the content is not used to train any model, and is not retained beyond the request save for a limited abuse-review window. The categories of Personal Data involved are those the Controller's presenters and participants enter as question or answer text; no separate category is collected for this purpose.

Categories of Data Subjects: presenters (the Controller's users) and participants (the audience members joining events).

Categories of Personal Data: presenter name, email address, hashed password, IP address (transient, not stored); optional participant display name and email; session identifiers; billing identifiers (PayPal payer ID, subscription ID).

Special categories of data: none are knowingly processed. The Controller is responsible for ensuring no special-category data is introduced through free-text poll responses unless a separate lawful basis applies.

Processing operations: collection, storage, use (display to authorised parties), automated content classification and summarisation by a language model, transmission to Subprocessors for email/error-monitoring/payments/AI processing, erasure on request or schedule.

Annex C — Subprocessors

The current list of Subprocessors is maintained on our [Subprocessors page](#) and incorporated into this DPA by reference.