NUTMEG SELF-SERVICE DATA PROCESSING AGREEMENT

Account-bound schedule incorporating the Commission Article 28 standard contractual clauses

VERSION 2026-09-14 — AVAILABLE FROM 2026-09-14. This DPA is incorporated into the same-version Terms and applies automatically where a teacher/customer controls student, pupil or studio personal data processed by Nutmeg. It becomes effective for that controller at the genuine electronic-acceptance time recorded for the authenticated teacher account.

1. Document basis and selections

This DPA incorporates by reference the European Commission standard contractual clauses between controllers and processors adopted by Implementing Decision (EU) 2021/915, available at https://eur-lex.europa.eu/eli/dec_impl/2021/915/oj. The selections and Annex I–III information below complete those Clauses for Nutmeg. The Clauses prevail if this schedule conflicts with them.

Item	Selected position
Applicable law	GDPR (Regulation (EU) 2016/679).
Docking clause	Not selected.
Subprocessor authorisation	General written authorisation under Clause 7.7, Option 2.
Change notice	At least 14 days before the intended addition or replacement, by email and in-app notice; the controller retains the rights stated in the clauses.
Annex IV	Not used because specific authorisation under Clause 7.7, Option 1 is not selected. The general-authorisation list appears in Schedule 1 below.

2. Parties — Annex I

Party	Identity and contact details supplied by the agreement and account record
Controller	The customer that controls the student, pupil or studio personal data: the individual teacher using the authenticated Nutmeg account, or the teaching organisation on whose behalf that person accepts the Terms and has authority to bind it. The party is identified by the account holder, verified account email, internal account identifier and any customer/organisation name supplied through the account or contractual correspondence. Nutmeg does not invent missing organisation details.
Processor	Marcin Sobieraj, sole trader (JDG) NIP 7831900655 Piaskowa 6 lok. 26, 61-753 Poznań, Poland hello@usenutmeg.com

Controller acceptance: the authenticated teacher submits the single Terms/Privacy/DPA acknowledgment during signup or the first-publication acknowledgment.

Processor acceptance: Nutmeg offers this DPA with the Terms and provides the service after valid electronic acceptance.

Agreement/effective date: the genuine server-recorded acceptance timestamp associated with the teacher account. It is never backfilled or inferred from earlier use.

DPA version: the same immutable 2026-09-14 version as the stored Terms version; the Privacy Policy version acknowledged in the same action is recorded separately.

3. Description of processing — Annex II

Field	Nutmeg schedule
Subject matter	Hosting and operating the Nutmeg music-practice workspace on behalf of the teacher/controller, including student records, lessons, practice assignments, communications, media and related studio administration selected by the controller.
Documented instructions	Provide the features selected by the controller; make data available only to authenticated and authorised users connected to the controller's studio; send controller-directed invitations and service messages; process uploaded media; support exports, corrections and deletions; and perform the security, support and deletion steps described in this schedule and the Nutmeg product. Nutmeg will notify the controller if an instruction appears to infringe applicable data-protection law, as required by the clauses.
Purposes	Studio and student administration; lesson and practice planning; progress recording; teacher-student communication; media storage and delivery; optional teacher-connected calendar functions; payment-status administration and sandbox payment testing; support, security and service reliability.
Nature of processing	Collection, recording, organisation, structuring, storage, retrieval, consultation, use, transmission to authorised users and agreed providers, restriction, export, correction and deletion.
Duration	For the duration of the controller's use of Nutmeg and afterwards only for the deletion/return process, provider operating cycles, or a documented legal, security or claims purpose. Approved deletion requests normally remove active account data within 30 days.
Frequency	Continuous or as initiated by authorised users while the service is used.

4. Data subjects and data categories

The categories below fall within this schedule only when Nutmeg processes them on the teacher/controller's documented instructions. Nutmeg's records of teacher legal acknowledgment, raw Google OAuth tokens used for a teacher-connected account, and separate authentication, account-security, abuse-prevention, legal-compliance and product-diagnostic evidence are processed for Nutmeg's own purposes and are outside this processor scope.

Category	Description
Data subjects	The controller/teacher; invited or teacher-recorded students, including children; authorised staff or collaborators if later enabled; message correspondents and persons appearing in teaching media. Parent login is not part of the current beta.
Invited-user identity and access data	Names, email addresses, user roles, locale, time zone, avatars and authentication identifiers needed to provide invited-user access on the controller's instructions.
Student and studio data	Instrument, teacher-entered optional birthday and student-since date, studio settings, notes, lesson rates and teaching relationship.
Teaching activity	Lessons, schedules, pieces, assignments, practice progress, ratings, goals, todos, comments and annotations.
Communications and media	Messages and uploaded images, documents, audio and video, including a student's voice or appearance.
Integration and payment data	Selected Google Calendar and event-mapping teaching data; manual payment records and Stripe sandbox identifiers/status when the controller selects those features.
Technical data	Technical events and provider object references generated while delivering controller-directed teaching features, including related device/network and access data. Nutmeg's separate account-security, abuse-prevention, legal-compliance and product-diagnostic evidence is outside this processor scope.

5. Special-category and high-risk content

Nutmeg is not designed to require health, biometric, religious or other special-category data. The controller must not enter such data unless it has documented necessity, a lawful basis and appropriate safeguards. Free-text notes, messages and media may nevertheless contain sensitive information. Safeguards include purpose limitation, controller-managed access, role and tenant checks, transport encryption, restricted operational access, diagnostic scrubbing and deletion handling. Direct/login-enabled accounts are prohibited for anyone known to be under 13; limited non-login student records may be maintained by an authorised teacher.

6. Technical and organisational measures — Annex III

Measure	Implementation
Transport protection	HTTPS/TLS is used for application and provider communications. Secrets and one-time authentication proofs are not placed in URL query parameters.

Measure	Implementation
Authentication	Supabase Auth provides Google OAuth and magic-link authentication. Invitation intents used to create controller-directed invited-user access use hashed secrets, one-hour expiry, attempt limits, email binding where applicable and conditional one-time consumption.
Authorisation and isolation	Server routes authenticate the session, validate input and enforce role and tenant ownership before access or mutation. Students are limited to their own teacher-linked records; parents are not enabled in the beta.
Administrative access	Provider and database administration is limited to operator-controlled accounts and credentials. Provider secrets are held in server environment configuration and are not sent to the browser unless explicitly designed as public, write-only identifiers.
Data minimisation	The product separates required and optional fields. Date of birth is not collected solely to enforce the under-13 rule. Users are instructed not to place unnecessary sensitive data in free text or uploads.
Media controls	Uploads use server-authorised provider references and validated formats/size limits. Supabase Storage and Bunny references are checked before use, Bunny delivery URLs can be signed where configured, and deletion workflows target exact provider objects.
Monitoring and diagnostics	Sentry is configured without default PII and application scrubbers remove sensitive keys, email-like text and URL values. For optional analytics, Nutmeg acts as controller and PostHog acts as Nutmeg's processor. That processing is opt-in only for public visitors and teachers, disabled for student and parent accounts, and outside the teacher/controller processing described in this schedule.
Abuse prevention	Rate limits and Cloudflare Turnstile protect selected authentication and invitation flows. Security failures do not create application accounts.
Resilience and recovery	Database backups, where configured, and provider recovery mechanisms support service recovery. Their availability, scope and operating cycles vary by provider and account configuration. Restored data must not be used to reverse a still-valid deletion.

Measure	Implementation
Deletion and incident handling	The operator uses documented account-deletion and under-13 response runbooks, records provider actions, keeps failed deletion cases open, and communicates a qualifying personal-data breach as required by the clauses.
Review and change control	Security and privacy behavior is covered by automated tests, legal-source validation and pre-release checks. Material provider or processing changes require review of this schedule and the provider/recipient inventory.

7. Return or deletion

At the controller’s choice and subject to Clause 10, Nutmeg will return an available account export or delete personal data after the services end, unless applicable law requires storage. A request is sent to hello@usenutmeg.com and may require reasonable identity and authority verification. Active account data is removed promptly after approval, normally within 30 days. Shared records and records for which another controller remains responsible are reviewed before deletion.

Deleted data may remain temporarily in database backups, where configured, or in provider recovery systems, caches and logs until overwritten or deleted under each system’s normal operating cycle. These systems differ by provider and configuration, are not used for ordinary product access and must not be used deliberately to reverse a valid deletion. Legal-acknowledgment, security, complaint and claims records are retained only for the documented purpose and applicable limitation period, not for an assumed universal fixed term. Cloudinary receives no new media and is not used for runtime delivery. It remains in Schedule 1 only while provider-managed backup or recovery copies await final removal or expiry under the provider's normal recovery lifecycle; Nutmeg does not claim an unverified fixed expiry period.

8. Assistance and requests

Nutmeg will provide reasonable assistance through hello@usenutmeg.com with data-subject requests, security information, breach handling, deletion/return and the controller’s compliance obligations described in the clauses, taking account of the nature of processing and information available to Nutmeg. The controller remains responsible for deciding and documenting its lawful basis, transparency information, authority over student records and responses to students or guardians where it is the controller.

9. General subprocessor authorisation

The controller gives general written authorisation for the subprocessors in Schedule 1. Nutmeg will give at least 14 days’ notice by email and in-app notice before an intended addition or replacement. The controller may object on reasonable data-protection grounds under the Commission clauses. Other material DPA or provider changes follow the notice process in the Terms. Existing acceptance is not treated as renewed agreement where the nature of a future change requires a fresh affirmative action. This section does not convert independent controllers or direct browser recipients into subprocessors.

Schedule 1 — Subprocessors under general authorisation

Provider	Processing for the controller	Location/transfer position
Supabase	Authentication, hosted application database and object storage for studio, lesson, message, billing and uploaded-media records.	Primary project data is hosted in Ireland. The Supabase Customer DPA is incorporated into its service agreement and provides the 2021 SCCs for relevant restricted transfers.

Provider	Processing for the controller	Location/transfer position
Vercel	Hosting, server execution and operational logs for the Nutmeg application.	Processing may occur in the United States and through Vercel's global infrastructure and subprocessors. Vercel's DPA applies to the covered services and provides the 2021 SCCs where required.
Resend	Authentication, invitation and transactional email sent for the controller's studio.	Customer email data is stored in the United States. Resend's DPA applies through account signup and uses the 2021 SCCs for applicable restricted transfers.
Cloudflare	Turnstile bot protection and routing of inbound support/service email.	Processing uses Cloudflare's global network and may include the United States. Cloudflare's DPA provides transfer safeguards, including the EU-US DPF and SCCs where applicable.
Sentry	Scrubbed error and performance monitoring needed to operate the service.	United States. Nutmeg accepted Sentry DPA version 5.1.0 on 11 September 2026. It uses the EU-US Data Privacy Framework and the 2021 SCCs where applicable. Event data is currently retained for 30 days; organisation audit logs follow a separate lifecycle.
bunny.net	Video processing, storage, playback and delivery telemetry.	Primary Stream storage is in Frankfurt, Germany, with replicas in Los Angeles, New York and Singapore; delivery uses a global CDN. Nutmeg has accepted BunnyWay d.o.o.'s Article 28 DPA. Under its DPA and applicable data-protection law, Bunny is responsible for appropriate safeguards when using a non-EEA subprocessor or network partner. No exact backup-expiry period is claimed.
Cloudinary (legacy/offboarding only)	Temporary retention of provider-managed backup or recovery copies of some previously migrated images, documents and audio. No new uploads, runtime reads or media delivery.	Cloudinary-managed global cloud and recovery infrastructure; Nutmeg does not select the location of residual recovery copies. Cloudinary's published privacy and DPA terms describe the 2021 SCCs and other safeguards where required. Residual copies await final removal or expiry under

Provider	Processing for the controller	Location/transfer position
		the provider's normal recovery lifecycle; no unverified fixed expiry period is claimed.

Not included as subprocessors in this schedule: Stripe and Google can act as independent or mixed-role recipients for their selected services; DiceBear, YouTube and Vimeo receive direct browser requests; for Nutmeg's optional analytics, Nutmeg acts as controller and PostHog acts as Nutmeg's processor, outside the processing performed for the teacher/controller under this schedule; analytics is disabled for student and parent accounts; Proton and Anthropic are dormant.

Electronic acceptance record

Field	Value supplied by the account and acceptance record
Controller legal identity and contact	The customer/controller described in section 2, identified through the authenticated teacher account and service relationship.
Controller representative/contact person	The authenticated account holder; where acting for an organisation, the account holder confirms authority to bind it.
Agreement/effective date	The actual server-recorded timestamp of the teacher's electronic acceptance.
Method and record of acceptance/signature	Single checked acknowledgment; the stored Terms version identifies both the accepted Terms and same-version DPA, while the acknowledged Privacy Policy version is recorded separately.
Controller-specific written instructions or restrictions	Standard Nutmeg configuration and the instructions in this DPA; additional restrictions apply only if separately agreed in writing.