Privacy Policy

Version 11
Effective 27 October 2026
Published 27 October 2026

Ventla
Apple App Store developer: Ventla International AB
Google Play developer: Ventla International AB

Controller for platform/account data: Ventla International AB, Org. nr 559081-9941, Nellickevägen 26, 412 63 Göteborg, Sweden.

Privacy contact: dataprivacy@ventla.com

This Privacy Policy explains how Ventla International AB ("Ventla", "we", "us") handles personal data in connection with the Ventla event platform, including our administrator web app, mobile apps, scanner/portal, and event websites (together, the "Platform"). It applies to everyone with a Ventla account, whether you are an event organizer (administrator) or an event participant.

1. The two roles: who is responsible for your data

Ventla is a technology provider. How we act under data-protection law depends on which data is involved:

- Event and participant data, the organizer is the controller, Ventla is the processor. When an organizer creates an event and adds, imports, or invites participants and stages event content, the organizer decides what data is collected and why. Ventla processes that data only on the organizer's instructions to run the event. If you are a participant and want to exercise your rights over your event data (access, correction, deletion, objection), please contact the organizer of your event first; we will assist them as their processor.
- Account and platform-operation data, Ventla is the controller. For the data we need to provide, secure, and operate the Platform itself, your login credentials and security tokens, sign-in and consent records, internal account-management notes about customer organizations and their administrators, and platform integrity/audit logs, Ventla is the controller and this Policy governs directly.

This split is mirrored in the Data Processing Agreement we offer to organizers, under which the organizer is the controller and Ventla is the processor for event and participant data.

If an organizer chooses to connect an AI client to their event data (see section 2, "AI access to event data"), the organizer remains the controller for that access, and the AI client the organizer connects is the organizer's own tool, not a Ventla sub-processor.

2. What data we process

We do not collect more than the Platform needs to operate. Specifically:

Account and identity

- Email address; first and last name.
- Password, for administrators only, stored as a salted hash (bcrypt); never stored in readable form. Participants normally sign in without a password via a one-time email code or a personal sign-in link.
- Profile details you choose to add: profile photo, company, job title, short bio, social links, preferred app language.
- An optional phone number, if you give one or an organizer records one for you. Unlike company and job title, a phone number belongs to your account rather than to a single event, so the same number applies everywhere you use Ventla and is visible to the organizers of every event you take part in. You can see and change it in your profile at any time, or clear it entirely.
- Optional two-factor authentication (for administrators): a time-based one-time-password secret, encrypted at rest.
- Optional enterprise single sign-on (Microsoft Entra ID): your email, name, and the identifiers your

organization's directory returns when you choose to sign in with SSO.

Security and sign-in

• Hashed security tokens for sessions, password resets, one-time email sign-in codes, and participant sign-in links (we store only a hash, never the plain token).
• The IP address and browser/device user-agent at the moment you accept these terms or the Privacy Policy, recorded as proof of consent. We do not otherwise log your IP address for tracking.
• The time you last used the Platform (a last-activity timestamp), used only to enforce the retention period in section 5. We do not otherwise profile or track your activity.

Event participation (staged or collected by the organizer)

• Your participant record, attendance status, and registration/check-in activity.
• Answers to the organizer's registration form and custom questions, which can include free text, choices, dates, and file attachments the organizer asks for.
• Session RSVPs and bookmarks, group membership, and a private activity log of your event actions (e.g. registered, signed in, checked in, responded to a survey) that is visible to the organizer.
• Viewing time, if the event streams video through Ventla: how many minutes a day you watched each live stream or replay in the app, counted while it plays, so that streaming can be billed and reported on. Only the stream or video, the day and the number of minutes are recorded.
• An event-specific profile you can edit (photo, company, title, about, tagline, banner, social links, networking "looking for" categories), kept separately from your global account profile.
• Your phone number is not part of this event-specific profile: there is one number on your account, shared across events (see "Account and identity" above). What you set per event is who can see it. If you give a phone number, other attendees at the same event can see it by default, alongside your company and job title; you can hide it per event under Settings then Privacy in the app, at any time and as often as you like. Hiding it affects other attendees only: the organizer of an event you take part in can always see it, and can include it in a participant list they export.

Content you create in an event

• Activity-feed posts, comments, reactions, and any photos or videos you upload.
• Chat messages (one-to-one and group), image attachments, and reactions; chat blocks you set.
• Poll and survey responses (which an organizer may configure to be anonymous).
• Private lists you build (e.g. "leads", "met"), visible only to you, not to the people on them and not to organizers.

Notifications and preferences

• A push-notification token for your device (via Expo) and your per-event notification and privacy preferences.
• The language your device reports when we register your push token, stored as a language code only and used, together with your preferred app language, to pick the language of the system push notifications we send you. Your preferred app language also picks the language of the system emails we send you; the device-reported language is additionally used for event-related system emails (for example registration and cancellation notices), but not for sign-in codes or password resets.

Communications

• Email delivery and engagement events (sent, delivered, opened, clicked, bounced, marked as spam, or failed) for emails an organizer sends through the Platform, used to report delivery and let organizers manage their sends.
• An organization-level do-not-email (suppression) list that records an email address and why it must not be mailed (a hard bounce, a spam complaint, a one-click unsubscribe, or a manual block by an administrator), used to protect deliverability and to honor opt-outs across that organizer's events. Non-essential emails include a one-click unsubscribe link.
• If you are an administrator, an optional subscription to our product-update ("What's new") emails. This is off unless you opt in, and you can unsubscribe at any time.

Support and feedback

• When you submit a bug report, feedback, or support request from the in-app Help panel, we store (as

controller) your message and your name and email, together with technical context to help us reproduce and follow up: the page you were on, your organization and event, your app version, and your browser and device. You may attach up to five screenshots; a screenshot of a page you were working on can contain other people's personal data, so please attach only what is needed. Every submission is sent to our support inbox, with any screenshots attached, and the screenshots are also readable in the app by you and by our support team. We delete screenshots 180 days after you send them; the text of your submission is kept. Please do not include other people's personal data in a support message.

Account management (administrators)

• If you administer an organization, we (as controller) keep internal account notes and a log about your organization and its administrators for our customer relationship, for example your plan, purpose, and support history. These notes are for our staff and are not shown to you in the app, but you can ask us for a copy of the notes we hold about you.

AI access to event data (only if your organizer turns it on)

• An organizer can allow AI clients (for example an AI assistant such as ChatGPT, Claude, or Microsoft Copilot, or an AI tool the organizer runs itself) to reach their event and participant data through a secure programmatic interface. A client connects either with an access key the organizer issues, or with "Sign in with Ventla": the administrator signs in with their own account on a Ventla approval page that names the AI app and what it will be able to do, and approves or refuses the connection. This is off by default and controlled per organization: the organizer decides whether AI access is allowed at all and, if so, whether it is read-only or may also make changes, and grants access to specific named people. Both connection methods are subject to exactly the same limits.
• When enabled, a connected AI client can read the same event data the granted administrator can already see (participant names, email addresses and status, groups and segments, event content, and registration questions) and, where the organizer allows changes, add, update, or delete participants and event content, and add or change registration questions. Every change made this way is recorded in the organizer's audit trail and marked as made via an AI client.
• The organizer can turn on an option to mask email addresses in what AI clients read.
• The AI client is the organizer's own tool: Ventla exposes the data to the organizer's client on the organizer's instruction. Administrators can see the AI apps they have connected on their account page and disconnect any of them at any time, and access keys can likewise be revoked; either takes effect on the client's next request, as does switching AI access off or removing a person's grant. Ventla does not itself send your data to any AI provider and does not use your data to train AI models. Any access Ventla staff are granted to an organization's data for support is off by default, requires a recorded reason and a second person to authorize it, and is recorded in that organization's own audit trail.

Location

• Only the event's location as text, and, where an organizer adds a weather widget, the event venue's coordinates. We do not collect participants' device GPS or track your location.

What we do not process

• No payment or card data is processed in the Platform. Billing is handled separately and is outside this Policy.
• No third-party advertising or analytics trackers (e.g. Google Analytics, Meta, advertising SDKs) are embedded in the Platform.

3. Why we process it, and our legal bases

For data where Ventla is the controller (account/platform-operation data), we rely on:

• Performance of a contract / taking pre-contractual steps (Art. 6(1)(b) GDPR), to create and operate your account and provide the Platform.
• Legitimate interests (Art. 6(1)(f)), to keep the Platform secure, prevent abuse, debug, handle support and feedback requests, manage our customer relationship (including internal account notes about organizers), and keep records of consent and account-deletion as legal proof.
• Legal obligation (Art. 6(1)(c)), where we must retain certain records.

- Consent (Art. 6(1)(a)), for push notifications, our optional product-update ("What's new") emails to administrators, and any optional features you turn on. You can withdraw consent at any time; for product-update emails, use the unsubscribe link in every email.

For event and participant data, the organizer determines the legal basis as controller. Ventla processes it on their documented instructions.

4. Who we share data with (sub-processors)

We host the Platform on, and use a limited set of vetted service providers ("sub-processors"). Each is bound by a data-processing agreement and processes data only to provide its service to us.

Who at Ventla can see your data. Ventla's staff, and a small number of contracted support and administration personnel who work for us under a services contract, may access personal data to run the Platform, set up and troubleshoot events, and answer support requests. Some of them work from outside the EEA (today from India, see "International transfers" below). All of them work only inside Ventla's own systems, with accounts we issue and manage, under written confidentiality and our instructions, and none of them keep your data on systems of their own. Contracted personnel who work this way are our personnel for data-protection purposes, not sub-processors, so they do not appear in the table below.

- Google Cloud Platform (Google Ireland Limited; Cloud Run, Cloud SQL/PostgreSQL, Cloud Storage, Secret Manager, Certificate Manager, Cloud DNS)
  - Purpose: Hosting, database, file storage, secrets, and TLS certificates and DNS for event-website domains
  - Data involved: All Platform data
  - Location: EU, Sweden (Stockholm, europe-north2, for production; the Finland region, europe-north1, is used for staging only)
- Resend (Plus Five Five, Inc.)
  - Purpose: Sending transactional and event emails
  - Data involved: Recipient email, name, message content; delivery events
  - Location: United States
- Mux (Mux, Inc.)
  - Purpose: Video upload, processing, playback, and live streaming
  - Data involved: Videos uploaded to an event, and an event's live streams and their recordings (may show people)
  - Location: United States
- Expo (650 Industries, Inc.)
  - Purpose: Mobile push-notification delivery (routed to Apple APNs on iOS and Google Firebase Cloud Messaging on Android)
  - Data involved: Device push token, notification content
  - Location: United States
- Microsoft (Entra ID and Microsoft 365) (Microsoft Ireland Operations Limited)
  - Purpose: Optional enterprise single sign-on; and our own email, support inbox, and office tools
  - Data involved: For single sign-on: email, name, directory identifiers (only if SSO is used). For our email and support inbox: the name, email and content of messages you send us, including support requests from the in-app Help panel and any screenshots attached
  - Location: Microsoft global infrastructure
- Sentry (Functional Software, Inc., dba Sentry)
  - Purpose: Application error and crash monitoring (mobile app, web apps, and backend services)
  - Data involved: Diagnostic error/crash data: error messages, stack traces, device/browser and OS information, a pseudonymous user id, and a request id. Configured to exclude IP addresses, request bodies, and personal fields
  - Location: European Union (EU data region)
- HubSpot (HubSpot Ireland Limited)
  - Purpose: Customer relationship management (our sales and account relationship with event organizers)
  - Data involved: Organizer/customer contact details (name, business email, company); not event-participant data

    - Location: United States
- GitHub (GitHub, Inc.)
    - Purpose: Engineering and support triage of in-app bug, feedback, and support reports (kept in private repositories)
    - Data involved: Reporter name and email, the message, and technical context (page, organization, event, browser)
    - Location: United States
- Featurebase (Cordnet OÜ)
    - Purpose: Feedback and support portal where you can send us ideas, vote on suggestions, and ask for help. This runs alongside the in-app support form, which we handle ourselves.
    - Data involved: Name, email, and message content of people who contact us through it
    - Location: EU (Germany, the Netherlands, and Ireland)

Other services (no personal data). We also use a few third-party services that do not receive your personal data: Open-Meteo (OpenMeteo GmbH) for the weather widget (event location only), Unsplash (Unsplash Inc.) for stock-image search in the admin (organizer search terms only), and OpenStreetMap (OpenStreetMap Foundation) for venue map tiles on event websites (event location only).

International transfers. Our core infrastructure (hosting, database, storage) is in the EU (Sweden). Where a sub-processor processes personal data outside the EEA, the transfer is safeguarded by the EU-US Data Privacy Framework (DPF) for providers certified under it, and otherwise by the EU Standard Contractual Clauses with supplementary measures. Google, Microsoft, GitHub, HubSpot, Resend, Mux, and Expo are DPF-certified. Featurebase (Cordnet OÜ, established in Estonia) hosts entirely within the EEA (Germany, the Netherlands, and Ireland), so no third-country transfer arises for it. Our own staff and contracted personnel access personal data remotely from within the EEA (Sweden and France) and from India; this covers both the data we process for organizers (event and participant data) and the data we hold as controller (organizer contact details, support and email correspondence). No data is stored in India: access happens only inside our own systems, with named accounts, and signing in to the Platform's administration requires multi-factor authentication. For access from India we have entered into the EU Standard Contractual Clauses with the contracted party, keep a transfer impact assessment on file, and apply the supplementary measures described in section 6. We will update this section before anyone accesses personal data on our behalf from a further country outside the EEA without an EU adequacy decision.

We do not sell personal data and do not share it for advertising.

AI clients are not sub-processors. Where an organizer enables AI access to their event data (see section 2), the AI client is software the organizer chooses and runs, connecting to the Platform with keys the organizer issues or through connections its administrators individually approve and can revoke. Ventla does not select that client, control it, or send data to it of its own accord, so it is the organizer's own tool rather than a Ventla sub-processor, whichever way it connects. Ventla itself does not send your personal data to any AI provider and does not use it to train AI models.

Links to other sites. The Platform can show links to third-party websites (for example, an organizer's own pages, or links shared in the activity feed, news, or chat), and some open in an in-app browser for convenience. Those sites are outside our control and are governed by their own privacy policies; we are not responsible for their content or how they handle your data.

5. How long we keep data

- Maximum retention. We keep your personal data only as long as needed for the purposes above and, as a maximum, we delete or anonymize it no later than 14 months after you last use the Platform, unless a longer period is required by law or to establish, exercise, or defend legal claims. Before an inactive account is deleted we email you a reminder about a month beforehand, so you can keep your account simply by signing in.
- Account deletion. You can delete your account at any time in the app, or by emailing dataprivacy@ventla.com (see "How to delete your data" below). The account enters a 30-day recovery window (you can restore it by signing in during that time). After 30 days a background job permanently erases your account and personal data. Content you authored (feed posts, comments, chat messages) is anonymized, detached from your name, rather

than removed, so conversations others took part in stay intact.
• Event deletion. When an organizer deletes an event, it is moved to the organizer's archive, marked as deleted, where the organizer can restore it. The participant records for that event (participant profiles, registrations, answers, bookings, posts and messages, and the photos and videos in the event's galleries) are permanently deleted when the organizer deletes the event permanently (a second step, available to the organization's administrators), or removes the participants from it. The organizer's audit trail keeps a record of the administrative actions taken on the event, with the participants' names removed.
• Security tokens are short-lived: sign-in sessions ~15 minutes (refreshing up to 7 days), password-reset links 1 hour, one-time email codes ~10 minutes, participant sign-in links up to 12 months, participant registration-management links until the form closes or the event ends, and administrator preview links within hours. All are stored only as a hash.
• Viewing time is deleted when you are removed from the event or your account is deleted, and after thirteen months at the latest.
• Do-not-email records. If you unsubscribe, your email hard-bounces, or you mark an organizer's mail as spam, we keep a minimal do-not-contact record (your email address and the reason) so we can keep honoring that choice. We keep it even after your account is deleted, and we use it for no other purpose.
• Support and feedback records. When you submit a bug report, feedback, or support request, we keep your message, name, email, and technical context in our support and engineering systems (including GitHub) to resolve it and improve the Platform. Screenshots you attach are deleted automatically 180 days after you send them, and are never copied into GitHub: the engineering record holds only a link that stops working once they are deleted. The message text itself is kept. When you delete your account, we remove or anonymize the personal details in these records, and your screenshots are deleted with them, consistent with how we anonymize other content you author; you can also ask us to delete a specific request.
• Consent and deletion records. Records proving you accepted these terms, and the account-deletion audit log, are kept as legal proof; your identifier is anonymized when your account is erased.
• Backups. Production databases have automated daily backups with point-in-time recovery and a 7-day transaction-log retention window, for disaster recovery.

6. How we protect data

• Encryption in transit (HTTPS/TLS) everywhere, and encryption at rest for the database and file storage (provider-managed).
• Passwords are bcrypt-hashed; security tokens are stored only as hashes; the two-factor secret is additionally encrypted.
• Uploaded media is served via short-lived signed URLs.
• Secrets are held in a managed secrets vault; our core data stays in the EU.
• Access is role-based and tenant-isolated so one organization cannot see another's data.
• Everyone who works with data on our behalf, employee or contractor, uses a named account we issue and loses that access on the day they leave; signing in to the Platform's administration requires multi-factor authentication. Access is role-based: the people who administer the Platform, including contracted personnel, can reach every organization's data in order to run it and give support. Significant changes made to an organization's event and participant data, including ours, are recorded in that organization's own audit trail with the name of the person who made them.
• Everyone with access is bound by written confidentiality, follows our documented instructions, completes our data-protection and security briefing before first access and yearly after that, works only from encrypted, locked, up-to-date devices, and never copies personal data out of our systems.

7. Your rights

Subject to applicable law, you have the right to access, correct, delete, restrict, object to, and port your personal data, and to withdraw consent.

• For participant/event data, contact your event organizer (the controller); we will support them in responding.
• For account/platform data, contact us at dataprivacy@ventla.com.

In the Platform you can already, for your account: edit your profile, control what other participants can see (hide selected fields, opt out of chat, opt out of being added to lists), mute notifications, export your own information, and request account deletion (with a 30-day restore window). You can also unsubscribe from an organizer's non-essential emails at any time using the one-click link in every such email; essential messages about your own registration may still be sent. You also have the right to lodge a complaint with the Swedish Authority for Privacy Protection (IMY) or your local supervisory authority.

How to delete your data. You can delete your personal data in any of these ways:

- In the app: open the menu, tap Account settings, then under Account deletion tap Delete account and confirm. Your account is signed out and enters a 30-day recovery window; after 30 days it is permanently erased.
- Online form: submit a request through our data-deletion request form at admin.ventla.com/legal/delete-request (no sign-in required).
- By email: write to dataprivacy@ventla.com and we will action your request.

8. Children

The Platform is not directed to children under 16, and we do not knowingly create accounts for them (16 is the default age of digital consent under Article 8 GDPR). Organizers running events that involve minors are responsible for an appropriate legal basis and any parental consent under their local law.

9. Changes to this Policy

When we update this Policy, the Platform assigns a new version automatically and records the effective date. Where the law requires, we will ask you to review and accept the new version.

10. Contact

Ventla International AB · Nellickevägen 26, 412 63 Göteborg, Sweden · Org. nr 559081-9941

Privacy and data-protection questions: dataprivacy@ventla.com