Privacy policy

Version 1.4 - In effect from 12 November 2026

What we collect, who else touches it, and how long we keep it - described specifically enough that you could check.

Two different people are described here

Schools buy Doras and decide what happens to their callers' information. In legal terms the school is the controller and we are its processor: we handle caller data on the school's instructions, not for our own purposes. The data processing addendum is where that is written down as a contract.

Callers are the people who ring a school's admissions line. They have no account with us and never agreed to anything with us. Most of this page is about them, because they are the people with the least say in it.

What we collect from a caller

When somebody calls a line Doras answers, we record the call and keep the audio, a transcript of it, the phone number they called from, the time and length of the call, and what the conversation was about - the programme they asked about, whether a tour was booked, whether they need calling back. If they give a name, an email or a funding source, we keep that too, because that is what the school needs to follow up.

Every call is announced as recorded before anything else happens, in every state, without exception. A caller who does not want to be recorded can hang up during the notice, and nothing is kept.

Callers are also told they are speaking with an assistant rather than a person.

If a caller texts the school, we keep the messages, the delivery status, and the record of what basis we had for sending anything outbound.

What we collect from a school's staff

A name, an email address, an optional mobile number, the role they hold, and when they were last signed in. Accounts exist by invitation only - nobody can sign themselves up - and sign-in is an email address and a password the person chooses when they accept. We keep a record of every change to who has access and who made it, and of every session a person holds, so that signing out of a device they no longer have is something they can do themselves.

Where recordings live

In a private bucket, never a public one. A recording is reachable only through a link we sign at the moment somebody with access asks for it, and that link stops working after fifteen minutes. There is no URL you can share, guess or index.

How long we keep it

Call audio is deleted after the retention period set on the school's account, which is twenty-four months unless

they have chosen something shorter. That deletion is real: the audio file leaves storage and the pointer to it is cleared. It is not hidden from a screen while sitting in a bucket.

Transcripts are kept longer than audio, and it is worth saying why rather than leaving it to be discovered. The transcript is what the call log, the reports and the accessibility of every recording are built on - a recording with no transcript is unusable by anybody who cannot hear it. Audio retention and record retention are different questions and this product answers them differently.

When a school closes its account, everything stays available to export for thirty days and is then deleted.

Who else touches it

We use other companies to run this service. Each one gets only what it needs to do its job.

Supabase - the database, sign-in and recording storage. Vercel - hosting. Retell - the voice agent that holds the conversation and, on a line whose number it hosts, the phone number and the call itself, which it carries through its own telephone carrier. Twilio - the phone numbers, the calls and the texts on the lines we carry on our own account. Anthropic - reads a finished transcript to work out what the call was about. OpenAI - turns questions into vectors so that two ways of asking the same thing are recognised as one gap. Google or Microsoft - only if the school connects a calendar, and only to read availability and write the bookings. Inngest - runs the scheduled work. Resend - sends email to school staff. Upstash - rate limiting. Stripe - billing. Stripe never receives caller data.

We do not sell information about callers, we do not share it for advertising, and one school's calls are never used to build anything for another.

What our error and analytics tools are not allowed to see

This is where most products leak, so it is written out rather than summarised. We use Sentry for errors and PostHog for product analytics, and both are deliberately blinded:

Transcripts are never sent to either. Not truncated, not sampled - removed before an event leaves the building.

Phone numbers are replaced before they leave. On our servers a number becomes a keyed one-way value, which lets us see that the same caller hit the same error four times without either vendor holding the number. In a browser it is removed outright.

Search terms go too. The call log's search box searches transcripts, so what somebody typed into it is a fragment of a phone call. It is stripped out of every error report and every analytics event.

Session replay is off, and so is click autocapture. Both record what is on screen, and the screens this product spends its day on show a caller's name, their number and what they said. Neither is enabled.

Text messages

A school texts somebody only when they have said yes. When the assistant takes a number on a call for a visit or a callback, it asks whether the school may text them a confirmation and a reminder, and their answer is kept with the call, the time and the exact words they were asked. The other way is a person texting the school first, who is answered in that conversation. Marketing texts are off unless a school has deliberately turned them on, and even then we never text somebody before 8am or after 8pm where they are, and never again once they have replied STOP. A STOP applies to every conversation with that school, not just the one it was sent in, and lasts until they reply START.

Mobile phone numbers and text messaging consent are never shared with third parties or affiliates for their

marketing or promotional purposes.

Security

Each school's data is isolated in the database itself, not by application code remembering to filter - a query that forgot would return nothing rather than somebody else's calls. Calendar credentials are encrypted where they are stored. Passwords are held by our authentication provider, never by us, and are checked against a public breach corpus when they are set.

When our staff open a school's account to help, the entry is recorded - who, when, why, and whose screen. The school can read that record itself, and anyone inside an account on our behalf is shown a banner they cannot dismiss.

Your choices

If you are a caller, you can ask the school you rang for a copy of what was kept about you, or ask them to delete it. They decide, because it is their record; we give them a way to find everything tied to one phone number and remove it, and we act on their instruction. If you would rather not be recorded at all, hang up during the notice at the start of the call and nothing is kept. Reply STOP to any text to stop all of them.

If you are a school, everything is exportable from the portal at any time, the retention period is yours to shorten, and you can ask us to close an account outright from Settings.

Children

This service is for people enquiring about post-secondary training and is not directed at children under 13. We do not knowingly keep information about them, and will delete it if a school tells us we have.

Changes to this page

We will tell schools by email at least thirty days before a change that affects what we do with their callers' information. The date at the top is when this text last changed.

Reaching us

privacy@doras.ai (privacy@doras.ai). If you are a caller and are not sure which school you rang, tell us the number you dialled and we will find them for you.
