Data processing addendum

Version 0.3 - Drafted 27 October 2026

DRAFT - NOT IN FORCE
This document has not been reviewed by counsel and no school has been asked to accept it. It is circulated so that it can be read and challenged.

The school is the controller, we are its processor, and this is that sentence in contractual form - with the annexes procurement reads.

1. What this addendum is, and what it attaches to

This data processing addendum forms part of the agreement between Doras and the school or organization identified in that agreement ("you"). Where this addendum and the terms of service disagree about the handling of personal information, this addendum governs.

It exists because of one distinction, which the privacy policy describes in plain words and which this document puts in contractual form: the information Doras handles about the people who ring your admissions line is yours, not ours. You decide what happens to it. We act on your instructions.

2. The roles

You are the controller of the personal information described in Annex A. You decide why it is collected and what is done with it.

Doras is your processor. We process that information only to provide the service, only on your documented instructions, and for no purpose of our own. Your use of the product - the settings you choose, the retention period you set, the exports and deletions you ask for - constitutes those instructions, together with anything you tell us in writing.

We will tell you if an instruction from you appears to us to break the law, and we may decline to act on it until it is resolved.

3. What we will not do with it

- We do not sell personal information, and we do not share it for advertising or

cross-context behavioural advertising.

- We do not use one customer's data to build, train, tune or evaluate anything

for another customer, or for ourselves.

- We do not retain, use or disclose personal information outside the direct

business relationship described in the agreement.

These are the certifications a service provider gives under the California Consumer Privacy Act as amended, and the equivalent provisions of the other US state privacy statutes. They are made here and they are made in the terms.

4. Confidentiality

Everyone at Doras who can reach your data is bound by confidentiality obligations that survive the end of their engagement, and reaches it only where their work requires it. Every entry by our staff into your account is recorded - who, when, why, and whose screen they were looking at - and that record is readable by you from your own Settings screen rather than on request from us.

5. Security

We maintain technical and organisational measures appropriate to the information. The measures in force are listed in Annex C. They may change as the product changes; they will not be weakened.

6. Sub-processors

You authorise the sub-processors listed in Annex B. Each receives only what it needs to perform its function, and each is bound by obligations no less protective than those in this addendum.

We will give you at least thirty days' notice by email to the account's owners before adding a sub-processor that will process personal information about your callers. If you object on reasonable data-protection grounds within that period we will work with you to find an alternative, and if there is none you may terminate the affected service without penalty under clause 3 of the terms.

We remain responsible to you for a sub-processor's performance as we are for our own.

7. Helping you answer the people you hold data about

Where somebody exercises a right you owe them - access, correction, deletion, knowing what was collected - the request is yours to answer, because it is your record. We will help, and the product is built so that most of the help is self-service: you can find everything tied to one phone number and remove it, and you can export any of it at any time.

If such a request reaches us directly, we will not answer it on your behalf. We will pass it to you promptly, and tell the person we have done so.

8. If something goes wrong

We will tell you without undue delay, and in any event within seventy-two hours, of becoming aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal information we process for you.

That notice will say what we know at the time: what happened, which categories of information and roughly how many records are affected, what we are doing about it, and who to speak to. We will keep telling you as we learn more, and we will not wait until the picture is complete before the first notice.

9. Deletion and return

Personal information is deleted on the schedule you set. Call audio is deleted after the retention period on your account - twenty-four months unless you have chosen something shorter - and that deletion is real: the file leaves storage.

When the agreement ends, everything remains exportable by you for thirty days. After that we delete it, except where we are required by law to keep something, in which case we keep only that and only for as long as we

must.

10. Audits and evidence

On reasonable notice, and no more than once in any twelve-month period unless a breach or a regulator requires otherwise, we will give you the information you reasonably need to satisfy yourself that we are meeting this addendum: our security documentation, the sub-processor list, our accessibility conformance report, and written answers to a security questionnaire.

11. Where the data is

All processing takes place in the United States. If that ever changes we will tell you before it does, under the notice period in clause 6.

12. Students and education records

Most of what this product handles is about people enquiring about a programme, who are not students. Where information we hold on your behalf forms part of an education record, you remain responsible for your obligations under the Family Educational Rights and Privacy Act, and we will act only on your instructions in relation to it.

This clause is under review. Whether Doras is a "school official" with a "legitimate educational interest" for the purposes of 34 CFR 99.31 is a question we have put to counsel and have not yet had answered, and this draft should not be relied on for it.

13. Liability

Each party's liability under this addendum is subject to the limitations and exclusions in the agreement.

14. Reaching us

Write to privacy@doras.ai (privacy@doras.ai) with an instruction, an objection to a sub-processor or anything else under this addendum, or raise it from the Support screen in your portal, which puts it in front of us with your account already attached.

Annex A - what is processed

Subject matter. Provision of an automated voice agent that answers your admissions line, and of the portal through which your staff work the calls it takes.

Duration. For as long as the agreement is in force, plus the thirty-day export window described in clause 9.

Nature and purpose. Answering, recording and transcribing inbound calls; identifying what each caller wanted; creating and updating a record of that person for you; booking appointments into your calendar; sending and receiving text messages on your behalf; and producing reports for you from all of it.

Categories of data subject. People who call or text your admissions line. Members of your own staff who hold accounts.

Categories of personal information.

ABOUT - WHAT

Callers

Phone number, name where given, email where given, the audio of the call, a transcript of it, the time and length of the call, what they asked about, how they intend to pay where they said, appointments booked, text messages exchanged, and any note your staff add

Your staff

Name, email address, optional mobile number, role, when they were last signed in, the devices holding a current session, and a record of every change to who has access

Special categories. None are asked for. A caller may volunteer something sensitive in the course of a conversation, as a caller may to any receptionist; nothing in the product solicits it, and it is handled under the same retention and access rules as the rest of the transcript.

Annex B - sub-processors

SUB-PROCESSOR - WHAT IT DOES - PERSONAL INFORMATION IT RECEIVES

Supabase

What it does: Database, authentication and recording storage
Personal information it receives: All of Annex A

Vercel

What it does: Application hosting
Personal information it receives: All of Annex A, in transit

Retell

What it does: Runs the voice conversation. On a line whose number it hosts, also provides the phone number and carries the call, through its own telephone carrier
Personal information it receives: Call audio and transcript; on those lines, also phone numbers and call metadata

Twilio

What it does: Phone numbers, calls and text messages, on the lines we carry on our own account
Personal information it receives: Phone numbers, call metadata, message content

Anthropic

What it does: Reads a finished transcript to determine what the call was about
Personal information it receives: Transcript

OpenAI

What it does: Turns questions into vectors so that two ways of asking the same thing are recognised as one
Personal information it receives: Question text

Google or Microsoft

What it does: Only where you connect a calendar: reads availability and writes bookings
Personal information it receives: Appointment details, caller name

Inngest

What it does: Runs scheduled work
Personal information it receives: Job payloads, which may reference records by id

Resend

What it does: Sends email to your staff
Personal information it receives: Staff name and email address

Upstash

What it does: Rate limiting
Personal information it receives: Hashed identifiers

Stripe

What it does: Billing

Personal information it receives: Your billing contact. No caller data.

Annex C - security measures

- Tenant isolation in the database itself. Every table carries row-level

security keyed on membership. A query that forgot to filter returns nothing rather than another school's calls.

- Recordings in private storage. Reachable only through a link signed at the

moment somebody with access asks for it, which stops working after fifteen minutes. There is no URL to share, guess or index.

- Encryption. In transit everywhere. Calendar credentials are encrypted at

rest with a key held outside the database.

- Authentication. Invitation only; nobody can create an account. Passwords are

held by the authentication provider, never by us, are checked against a public breach corpus when set, and every session a person holds is visible to them and endable by them.

- Least privilege by role. Four roles, with reading a recording separated from

reading the call log, because a recording is somebody's voice.

- Everything consequential is logged. Access grants, role changes, recording

access, exports, and every entry by our staff into your account, in a table nobody - including us - can edit.

- Observability is blinded. Transcripts are never sent to our error or

analytics vendors, phone numbers are replaced with keyed one-way values before they leave, session replay and click autocapture are off.

- Dependencies and egress are gated in the build. A new outbound destination

fails the test suite rather than appearing in production.