Privacy Policy

Core listens to your meetings, so we hold ourselves to a high standard. This is exactly what we collect, why, where it goes and how you stay in control.

LAST UPDATED

18 November 2026

COVERS

Core Mobile, Core, Core Mini and coremeeting.ch

PRIVACY CONTACT

contact@coremeeting.ch

01 The short version

Core listens to your meetings so it can write the notes, track what was agreed and follow up. That means we handle sensitive material, and this policy explains exactly what we collect, why, where it goes and how you stay in control.

ONLY WHEN YOU ASK

Core only records when you start a session, from the app, a calendar reminder or the button on a Core device. A visible indicator shows whenever it is listening.

STORED IN SWITZERLAND

Your meeting content is stored in Switzerland, with Infomaniak. It is transcribed and summarised by open AI models that Infomaniak runs for us in Switzerland. Two steps go through other providers, named in section 7: voice recognition (RunPod) and voice messages to Cora (Mistral AI).

NEVER SOLD

We do not sell your data or use it for advertising, and we do not track you across other companies' apps or websites.

NO TRAINING

We do not train any AI model on your meetings, and our AI providers commit not to either.

VOICE PROFILES

Core keeps a voice profile only of people who have agreed, in series where voice recognition is on, so it can recognise them in your later meetings. It is used for nothing else, and you must have everyone's agreement before recording.

AUDIO DELETED

A meeting's audio is deleted 24 hours after its notes are written, unless you choose to keep the recordings of a series.

ALWAYS DELETABLE

You can delete your meetings and your account from inside the app at any time.

02 Who we are

Core is operated by Nicolas Gauthier, Chemin des Coccinelles 9, 3963 Crans-Montana, Switzerland ("Core", "we", "us"). We are the controller of the personal data described in this policy, except where section 6 says we act as a processor.

Privacy contact: contact@coremeeting.ch

This policy covers the Core Mobile app (including beta versions distributed through TestFlight), the Core and Core Mini devices, and the website coremeeting.ch. It is written to meet the Swiss Federal Act on Data Protection (FADP), the EU General Data Protection Regulation (GDPR) and the UK GDPR, where they apply.

03 What we collect

We collect only what Core needs to work. Nothing below is collected until you create an account, join the waitlist or grant the relevant permission.

Account

WHAT IT INCLUDES

Name, work email, company, language, notification settings

WHERE IT COMES FROM

You

Meeting audio

WHAT IT INCLUDES

Sound captured by your phone’s microphone, or by a Core or Core Mini device, during a session

WHERE IT COMES FROM

Microphone, with your permission

Transcripts and notes

WHAT IT INCLUDES

Text of what was said, which speaker said it, summaries, decisions, commitments, owners and deadlines

WHERE IT COMES FROM

Produced by Core from the audio

Speaker labels

WHAT IT INCLUDES

Voice profiles used to recognise each speaker, and the names you or your calendar attach to them

WHERE IT COMES FROM

Audio, calendar, you

Calendar

WHAT IT INCLUDES

Meeting titles, times, locations, organiser and attendee names and email addresses

WHERE IT COMES FROM

Calendar access or a connected calendar account, with your permission

Photos

WHAT IT INCLUDES

Pictures you take or attach during a meeting, such as a whiteboard

WHERE IT COMES FROM

Camera or photo picker, with your permission

Phone motion

WHAT IT INCLUDES

Moments when the group stops or changes floor during a site visit

WHERE IT COMES FROM

iPhone motion sensors, with your permission

Companies and contacts

WHAT IT INCLUDES

Names, emails and phone numbers of the companies and people you add to a series or to your workspace

WHERE IT COMES FROM

You

Meeting memory

WHAT IT INCLUDES

The running record of people, open items and changes across your meetings

WHERE IT COMES FROM

Produced by Core from your meetings

Assistant requests

WHAT IT INCLUDES

Questions you ask Core, in writing or out loud, and the answers it gives

WHERE IT COMES FROM

You

Connected tools

WHAT IT INCLUDES

Access tokens and the content needed to carry out actions you request in tools you connect (Trello today)

WHERE IT COMES FROM

The tools you choose to connect

Device and diagnostics

WHAT IT INCLUDES

Device model, OS version, app version, language, crash logs, performance data, push notification token, Core device serial number and firmware

WHERE IT COMES FROM

The app and device

Support and feedback

WHAT IT INCLUDES

Messages you send us, TestFlight feedback and screenshots

WHERE IT COMES FROM

You, Apple

Waitlist

WHAT IT INCLUDES

First name, company, work email, products of interest, how you meet, tools you use

WHERE IT COMES FROM

The form on coremeeting.ch

We do not collect precise location, health data, contacts from your address book, advertising identifiers or payment card numbers. Diagnostics and usage statistics are collected by our own in-house system on our own servers; we use no third-party analytics, advertising or tracking tools in the app or on the website.

Voice profiles

To attribute each line to the right person, Core tells voices apart in series where voice recognition is on. It keeps a person's voice profile only if that person has agreed. The profile of a voice that nobody has named with the person's agreement is deleted after 30 days. Each profile belongs to one Core workspace, which is a single account or an organisation and its members, and is used only to recognise the same person in that workspace's later meetings. Profiles are never matched or shared across workspaces. Voice profiles are stored on our servers in Switzerland and are biometric data. To compute them, the meeting audio is processed by RunPod (section 7). We use them only to attribute notes: not to identify people for any other purpose, not for AI training, and we never share them. The account holder must have each participant's explicit consent before recording them with Core, and the app reminds you of this on first use. Anyone can ask to have their voice profile deleted by writing to us. Withdrawing a person's agreement in the app deletes their profile straight away.

04 How we use it, and on what basis

Record, transcribe and attribute meetings; write notes; track decisions and open items

DATA USED

Audio, transcripts, speaker labels, photos, calendar, phone motion

LEGAL BASIS

Performance of our contract with you

Recognise returning speakers across meetings

DATA USED

Voice profiles

LEGAL BASIS

Explicit consent

Keep the audio recording after notes are produced, when the series is set to do so

DATA USED

Audio

LEGAL BASIS

Consent, which you can withdraw at any time

Share notes and follow-ups with attendees, in their Core app, through a link to the online notes or from your own email, when you choose to

DATA USED

Notes, attendee names and emails

LEGAL BASIS

Performance of contract; our and your legitimate interest in sharing a meeting record with the people who were there

Send a follow-up to someone about a task, when you approve it

DATA USED

Follow-up text, recipient's name and email

LEGAL BASIS

Performance of contract, on your instruction

Let you know by email that your notes are ready

DATA USED

Account email, notes title and link

LEGAL BASIS

Performance of contract

Answer your questions about past meetings

DATA USED

Meeting memory, assistant requests

LEGAL BASIS

Performance of contract

Act in tools you connect

DATA USED

Connected-tool data

LEGAL BASIS

Performance of contract, on your instruction

Create and secure your account, prevent abuse

DATA USED

Account, device data

LEGAL BASIS

Performance of contract; legitimate interest in security

Fix bugs and improve reliability

DATA USED

Diagnostics, crash logs, feedback

LEGAL BASIS

Legitimate interest; consent where the law requires it

Email waitlist and product updates

DATA USED

Waitlist data

LEGAL BASIS

Consent, which you can withdraw with one click

Meet legal obligations

DATA USED

As required

LEGAL BASIS

Legal obligation

Under Swiss law we process personal data in line with the FADP principles of good faith, proportionality and purpose limitation. We do not use your data for a new purpose without telling you and, where required, asking first.

We do not sell personal data, show advertising, build advertising profiles, or make decisions about you by automated means that have legal or similarly significant effects.

05 Recording, and the other people in the room

Core never records in secret. The app asks for microphone permission before first use, shows a clear indicator for the whole time it is listening, and lets you pause or stop at any moment. Core and Core Mini devices show a light while they are capturing.

A meeting includes people who may not be Core users. If you use Core, you must tell everyone present that the meeting is being recorded and that Core recognises speakers' voices, and you must have their agreement before you start. The app reminds you of this on first use. For appointment series, it asks you to confirm before each recording. In Switzerland and many other countries, recording a private conversation without the consent of everyone taking part can be a criminal offence.

If you took part in a meeting captured by Core and are not a Core user:

- You may receive the notes, in the Core app, through a link to the online notes or by email from the organiser's own email, because the organiser chose to share them with attendees.
- If a task is assigned to you, you may receive a follow-up by email. Core sends it on the organiser's behalf from a Core address, and your reply goes straight to the organiser.
- You can ask the organiser, or us at the address in section 2, for access to, correction of, or deletion of what relates to you, including your voice profile. We will work with the account holder

to respond.

- We do not use your details to market Core to you.

Please do not use Core to capture special categories of data (such as health information) unless you have a lawful basis to do so.

06 Teams and organisations

When Core is used under an organisation's account, that organisation decides how meeting content is used and is the controller of it. We process that content on its behalf, as its processor, under our agreement with that organisation. Requests about such content are best sent to the organisation first; we will help it respond.

07 How AI is used

Core uses AI models to turn audio into text, attribute speakers, write notes, extract decisions and commitments, and answer your questions.

- Transcription, note-writing, Core's answers and reading photos use open models, such as Whisper, Mistral or Gemma, that Infomaniak runs for us in Switzerland as our processor.
- Voice recognition uses pyannote, run on RunPod's compute servers. The meeting audio is sent there for this computation.
- Voice messages you send to Cora are transcribed by Voxtral, at Mistral AI in France.
- We do not train any model on your meeting content, and our contracts with these providers forbid them from doing so. Data from tools you connect, such as your calendar or mailbox, is never used to train models.
- If we add an AI provider, we will name it here and tell you before sending it your data.

AI output can contain mistakes. Notes can be reviewed and edited, and you can set Core to hold notes for your approval before they are sent.

08 Who we share data with

We share personal data only in these cases:

Meeting attendees

Notes and follow-ups appear in the Core app of the people who attended, according to your settings. You can also send them from your own email, with a link to the online notes. Anyone with that link can read and edit the notes without an account: only pass it to the people concerned. Follow-ups

you approve are sent by email from a Core address, and replies come straight back to you. Nothing reaches anyone who was not at the meeting unless you choose to send it.

Tools you connect

When you connect a calendar, email, document, task, messaging or CRM tool, Core exchanges data with it to do what you ask. That provider's own privacy policy applies to the data it holds. You can disconnect any tool in Settings, which revokes Core's access.

Service providers

A small number of companies process data on our behalf under contracts that require the same level of protection as this policy and forbid any other use.

Legal reasons

Where we are required to by law or a binding order, or to protect the rights and safety of users and others. We will tell you unless we are legally prevented from doing so.

Business transfer

If Core is merged, acquired or reorganised, data may pass to the successor, which remains bound by this policy.

Infomaniak

PURPOSE

Application hosting and storage; AI transcription, note-writing, Core's answers and reading photos

LOCATION

- Switzerland

RunPod

PURPOSE

Voice recognition (GPU computation)

LOCATION

US company; data centres in several countries

Mistral AI

PURPOSE

Transcribing voice messages sent to Cora

LOCATION

France (EU)

Supabase

PURPOSE

Account sign-in and triggering account emails

LOCATION

Ireland (EU)

Brevo

PURPOSE

Delivering account emails (verification, sign-in codes), the "notes ready" email, follow-ups and product updates

LOCATION

France (EU)

Apple (TestFlight, push notifications)

PURPOSE

Beta distribution, feedback, notifications

LOCATION

USA and other countries

Core's use of information received from Google APIs adheres to the Google API Services User Data Policy, including its Limited Use requirements.

09 Where your data is stored

Meeting audio, transcripts, notes and meeting memory are stored on Infomaniak servers in Switzerland. Your sign-in details (email address and hashed password) are held by Supabase in Ireland, in the European Union.

For voice recognition, meeting audio is processed by RunPod, a US company, on servers that may be outside Switzerland and the EU. Voice messages sent to Cora are processed by Mistral AI in France.

Other service providers in section 8 may process limited data, such as email delivery records, TestFlight data and push notification delivery, outside Switzerland, the EEA and the UK. Where that country is not recognised as providing adequate protection, we rely on the European Commission's Standard Contractual Clauses, with the Swiss and UK addenda, or on the Swiss-US, EU-US and UK-US Data Privacy Framework where the recipient is certified.

10 How long we keep it

When you delete a meeting, it is removed from our live systems straight away. When you delete your account, we delete your account data and meeting content within 30 days, apart from what we must keep by law, such as accounting records. Notes already sent to attendees from your own email, and follow-ups already sent, stay in their inboxes; we cannot recall them.

Meeting audio

KEPT FOR

Deleted 24 hours after the first notes are written, unless you choose to keep the series' recordings. If you do, until you delete them or delete your account

Voice profiles

KEPT FOR

Only with the person's agreement. Until the person withdraws their agreement, the account holder or the speaker asks for deletion, or the account is deleted. The profile of a voice nobody has named with the person's agreement: 30 days

Transcripts, notes, photos, meeting memory

KEPT FOR

Until you delete them or delete your account

Account data

KEPT FOR

For as long as your account exists

Connected-tool tokens

KEPT FOR

Until you disconnect the tool or delete your account

Crash logs and diagnostics

KEPT FOR

Up to 12 months

Support messages and beta feedback

KEPT FOR

Up to 24 months

Waitlist data

KEPT FOR

Until you unsubscribe, or 12 months after launch

Backups

KEPT FOR

Overwritten within 30 days of deletion from live systems

11 Security

Data is encrypted in transit using TLS and encrypted at rest. Access to production systems is limited to the staff who need it, protected by multi-factor authentication, and logged. Core devices communicate with our servers over encrypted channels and receive signed firmware updates. A link to online notes is long and impossible to guess, and gives access to those notes only.

No system is perfectly secure. If a breach is likely to put your rights at risk, we will notify you and the competent authorities as the law requires.

12 Your choices and rights

In the app

Delete your account

Open the Account section and choose Delete account. This starts deletion of your account and all your meeting content, as described in section 10.

Delete a meeting

Open the meeting and choose Delete.

Recordings

In a series' settings, "Keep recordings" decides whether the audio is kept after the notes.

Voice profiles

In a series' voices, withdrawing a person's agreement deletes their profile.

Permissions

Microphone, camera, photos, calendar, Bluetooth, local network, motion and notifications can each be switched off in iOS Settings. Features that need a permission stop working without it; the rest of the app keeps working.

Connected tools

Disconnect any tool in Settings to revoke Core's access.

Emails

Every marketing email has a one-click unsubscribe link.

Under the law

Depending on where you live, you have the right to access your data, correct it, delete it, receive it in a portable format, restrict or object to our processing of it, and withdraw consent at any time without affecting what was done before. To use any of these rights, write to contact@coremeeting.ch. We reply within 30 days and do not charge a fee.

You can also complain to a data protection authority: in Switzerland the Federal Data Protection and Information Commissioner (FDPIC), in the EU your local supervisory authority, and in the UK the Information Commissioner's Office (ICO). We would appreciate the chance to put things right first.

13 Beta testing with TestFlight

If you test a beta version of Core through Apple's TestFlight, Apple shares with us your email address if you were invited by email, your device and OS details, crash logs, usage statistics for the beta, and any feedback or screenshots you choose to send. We use this only to find and fix problems. Apple's own handling of your data is covered by Apple's privacy policy and the TestFlight terms.

Beta versions may change or stop working, and content created during a test may be reset. You can stop testing at any time in the TestFlight app and delete your account as described in section 12.

14 Children

Core is a workplace product for people aged 18 and over. We do not knowingly collect personal data from children. If you believe a child has given us personal data, contact us and we will delete it.

15 Changes to this policy

We will update this policy when Core changes. The date at the top shows the latest version. If a change materially affects how we use your data, we will tell you in the app or by email before it takes

effect and, where required, ask for your consent again.

16 Contact

core

Nicolas Gauthier
Chemin des Coccinelles 9
3963 Crans-Montana, Switzerland

contact@coremeeting.ch