

Kuori Auth terms and privacy

- [Privacy policy](#)

Privacy policy

Kuori Oy is the controller for the personal data described here. Kuori Auth is the sign-in service for Kuori's applications, and Kuori runs it on its own servers. Its only job is to establish who you are. What an application does with your data after you have signed in is described in that application's own privacy policy, not here.

Questions about data privacy go to your Kuori representative or to signage@kuori.tech.

How you sign in

Kuori Auth hosts the sign-in page, so the applications never see your password or your code. There is no password to begin with. You sign in one of three ways:

- **An emailed code.** You enter your email address and we mail you a one-time code. It expires in 10 minutes and works once.
- **Google.** Google authenticates you and tells us your email address, name, and a link to your profile image. Google learns that you signed in to a Kuori service. What Google does with that is covered by Google's own privacy policy.
- **Your organisation's own single sign-on**, where your organisation has asked us to connect it. Your organisation authenticates you and sends us your email address and name. Its own privacy notice governs what it does.

You cannot create an account here. Identities exist because an application created one for you, and an application creates one only when someone entitled to grant you access does so.

What Kuori Auth stores

- Your identity. Email address, name, a link to your profile image, and the link to your Google account or to your organisation's single sign-on where you use one.
- Sign-in events. The time, the method, and the outcome. These records can contain your email address.
- Failed attempts, for lockout. Ten failed attempts within an hour lock the address for 10 minutes.

Nothing about what you are allowed to do is stored here. Roles, permissions and which organisation you work for belong to the applications.

What Kuori Auth tells an application about you

When you sign in to an application, it receives a permanent identifier for your identity, your email address, and a flag saying the address is verified. Your name and profile image link come along when the method you used provides them.

No role, permission, or organisation membership is ever carried in a sign-in token. Each application decides on its own what you may see and do, and refuses you if it has no record of you.

Sessions and cookies

Kuori Auth keeps a sign-in session in a cookie on its own address, which is what lets one sign-in serve several Kuori applications. Each application issues its own separate session and controls how long that lasts.

Signing out from inside an application ends that application's session and also ends the Kuori Auth session, so the next sign-in asks who you are again. Sessions that simply expire end only in the application.

How long we keep it

Your identity lives as long as at least one Kuori application uses it. A monthly job disables identities that no application uses any more and deletes them permanently 60 days after that. Deletion is final. If you return later, you are a new identity everywhere.

Database backups are deleted 30 days after they are taken, so a deleted record can survive in them until then, and no longer.

Sign-in event records have no automatic expiry today. We delete them on request as part of an erasure, and we are working on pruning them on a schedule.

Your rights

You can ask for a copy of the personal data we hold about you, ask us to correct it, or ask us to erase it. Erasure removes your records from every Kuori application and then permanently deletes

your identity here, without waiting for the monthly job. Backups taken before the request hold the older state until they age out 30 days later, and an application may keep records it has to keep for its own reasons, which its privacy policy explains.

Where we process your data on the basis of our legitimate interests, you can object to that processing under Article 21 and ask us to explain why our interest overrides yours in your case.

Send any of these requests to signage@kuori.tech. If you are not satisfied with how we handle one, you can complain to your national data protection authority. In Finland that is the Office of the Data Protection Ombudsman.

Sharing

Kuori Auth runs on Kuori's own infrastructure, so no external identity vendor holds your sign-in data. Google receives data only if you choose to sign in with Google, and your organisation's identity provider only if you sign in through it. Your data is not shared with anyone outside Kuori Oy for commercial purposes.