Security and trust

This is how we protect your data in NodeCE.

Last updated November 7, 2026

Where data is stored

- The cloud service runs at Hetzner in Helsinki, Finland.
- Data is stored within the EU/EEA, except email and error reports from the desktop app, which Resend stores in the USA.
- You can also run NodeCE on your own server.

Isolation

- A call is denied unless the role explicitly grants access.

Encryption

- All traffic to NodeCE from the browser and the app is encrypted. Email is encrypted when the recipient's server supports it.
- With self-hosting, backups are encrypted before they leave the server.
- The cloud service's server disks, database and database backups are encrypted when stored.

Backups

- The cloud service's database is backed up, and the copies are kept for no more than 30 days.

Access

- Users sign in with a passkey or a one-time code sent by email. NodeCE has no passwords for sign-in.
- You can require that everyone in the organisation has a passkey.
- Roles control what each user can see and do.
- The cloud service's database is reachable only by our operations staff, for operation, support and restoration.
- You can sign in via your own identity provider (SSO).

Logging

- The organisation's history shows who did what, including sign-ins.
- You can export your data and the history under section 9 of the Terms of Service.
- The history is sealed, so that changes made afterwards are detected.

Vulnerabilities and incidents

- We acknowledge every reported security weakness.
- In the event of a personal data incident, we notify you without undue delay.

Report a security weakness: https://www.nodece.se/en/security/ · Security advisories: https://www.nodece.se/en/security/advisories/

Software

- Every container image of the server software is signed and has a list of its components (SBOM).
- Every version is checked against known vulnerabilities before it is published.
- Published versions are checked regularly against new vulnerabilities.

Standards

- We keep a register of processing activities and a data processing agreement under the GDPR.
- Actively exploited vulnerabilities and serious incidents we report under Article 14 of the EU Cyber Resilience Act (CRA).
- Our routines are organised according to the controls in SS-EN ISO/IEC 27001 Annex A. We are not certified.

Subprocessors

- We notify you before a new subprocessor starts processing your data.

Our subprocessors: https://www.nodece.se/en/subprocessors/

We share our procedures and answers to security questionnaires under a non-disclosure agreement. kontakt@nodece.se