# Sikkerhet og tillit

Slik beskytter vi dataene deres i NodeCE.

Sist oppdatert 7. november 2026

## Hvor data lagres
- Skytjenesten kjører hos Hetzner i Helsingfors, Finland.
- Data lagres innenfor EU/EØS, unntatt e-post og feilrapporter fra skrivebordsappen, som Resend lagrer i USA.
- Dere kan også drifte NodeCE på deres egen server.

## Isolering
- Et kall avvises med mindre rollen uttrykkelig gir tilgang.

## Kryptering
- All trafikk til NodeCE fra nettleseren og appen er kryptert. E-post krypteres når mottakerens server støtter det.
- Med egen drift krypteres sikkerhetskopiene før de forlater serveren.
- Skytjenestens serverdisker, database og databasens sikkerhetskopier er kryptert når de lagres.

## Sikkerhetskopier
- Skytjenestens database sikkerhetskopieres, og kopiene oppbevares i maksimalt 30 dager.

## Tilgang
- Brukere logger inn med passkey eller med en engangskode på e-post. NodeCE har ingen passord for innlogging.
- Dere kan kreve at alle i organisasjonen har en passkey.
- Roller styrer hva hver bruker kan se og gjøre.
- Databasen i skytjenesten er bare tilgjengelig for våre driftsansvarlige, for drift, support og gjenoppretting.
- Dere kan logge inn via deres egen identitetsleverandør (SSO).

## Logging
- Organisasjonens historikk viser hvem som gjorde hva, også innlogginger.
- Dere kan eksportere deres data og historikken etter punkt 9 i de allmenne vilkårene.
- Historikken forsegles, slik at endringer i etterkant oppdages.

## Sårbarheter og hendelser
- Vi bekrefter hver rapporterte sikkerhetsbrist.
- Ved en hendelse med personopplysninger varsler vi dere uten unødig opphold.

Rapporter en sikkerhetsbrist: https://www.nodece.se/nb/security/ · Sikkerhetsvarsler: https://www.nodece.se/nb/security/advisories/

## Programvare
- Hvert containerbilde av serverprogramvaren er signert og har en liste over sine komponenter (SBOM).
- Hver versjon kontrolleres mot kjente sårbarheter før den publiseres.
- Publiserte versjoner kontrolleres jevnlig mot nye sårbarheter.

## Standarder
- Vi fører et register over behandlinger og en databehandleravtale etter personvernforordningen (GDPR).
- Aktivt utnyttede sårbarheter og alvorlige hendelser rapporterer vi etter artikkel 14 i EUs forordning om cyberresiliens (CRA).
- Våre rutiner er ordnet etter kontrollene i SS-EN ISO/IEC 27001 vedlegg A. Vi er ikke sertifisert.

## Underdatabehandlere
- Vi varsler dere før en ny underdatabehandler begynner å behandle deres data.

Våre underdatabehandlere: https://www.nodece.se/nb/subprocessors/

Våre rutiner og svar på sikkerhetsskjemaer deler vi under taushetsavtale. kontakt@nodece.se