Säkerhet och förtroende

Så skyddar vi era uppgifter i NodeCE.

Senast uppdaterad 7 november 2026

Var data finns
- Molntjänsten körs hos Hetzner i Helsingfors, Finland.
- Uppgifterna lagras inom EU/EES, utom e-post och felrapporter från skrivbordsappen, som Resend lagrar i USA.
- Ni kan också driva NodeCE på er egen server.

Isolering
- Ett anrop nekas om inte rollen uttryckligen ger åtkomst.

Kryptering
- All trafik till NodeCE från webbläsaren och appen är krypterad. E-post krypteras när mottagarens server stöder det.
- Med egen drift krypteras säkerhetskopiorna innan de lämnar servern.
- Molntjänstens serverdiskar, databas och databasens säkerhetskopior är krypterade när de lagras.

Säkerhetskopior
- Molntjänstens databas säkerhetskopieras, och kopiorna sparas i högst 30 dagar.

Åtkomst
- Användare loggar in med passkey eller med en engångskod via e-post. NodeCE har inga lösenord för inloggning.
- Ni kan kräva att alla i organisationen har en passkey.
- Roller styr vad varje användare får se och göra.
- Databasen i molntjänsten når bara våra driftansvariga, för drift, support och återställning.
- Ni kan logga in via er egen identitetsleverantör (SSO).

Loggning
- Organisationens historik visar vem som gjort vad, även inloggningar.
- Ni kan exportera era uppgifter och historiken enligt punkt 9 i de allmänna villkoren.
- Historiken förseglas, så att ändringar i efterhand upptäcks.

Sårbarheter och incidenter
- Vi bekräftar varje rapporterad säkerhetsbrist.
- Vid en personuppgiftsincident meddelar vi er utan onödigt dröjsmål.

Rapportera en säkerhetsbrist: https://www.nodece.se/security/ · Säkerhetsmeddelanden: https://www.nodece.se/security/advisories/

Programvara
- Varje containeravbild av serverprogramvaran är signerad och har en förteckning över sina komponenter (SBOM).
- Varje version kontrolleras mot kända sårbarheter innan den publiceras.
- Publicerade versioner kontrolleras regelbundet mot nya sårbarheter.

Standarder
- Vi har ett register över behandlingar och ett personuppgiftsbiträdesavtal enligt dataskyddsförordningen (GDPR).
- Aktivt utnyttjade sårbarheter och allvarliga incidenter rapporterar vi enligt artikel 14 i EU:s cyberresiliensförordning (CRA).
- Våra rutiner är ordnade efter kontrollerna i SS-EN ISO/IEC 27001 bilaga A. Vi är inte certifierade.

Underbiträden
- Vi meddelar er innan ett nytt underbiträde börjar behandla era uppgifter.

Våra underbiträden: https://www.nodece.se/subprocessors/

Våra rutiner och svar på säkerhetsfrågeformulär skickar vi under sekretessavtal. kontakt@nodece.se