



KAPITTEL 5

Fire nivåer av absolutt sikkerhet
(Datasikkerhet og personvern / GDPR)

Sikkerhet integrert i prosjektets DNA

"Security by Design"-konseptet. Hvorfor LINK AI er sikkert i sin natur.



Prioritet nr. 1

Sikkerhet er selve fundamentet i arkitekturen, ikke et tillegg på slutten.



Isolasjon

Prosjektet har ingen tilgang til UDIs lukkede servere eller Link AS sine interne databaser.



Autonomi

Systemet fungerer som en uavhengig, smart guide for praktiske spørsmål på mottaket.

ARKITEKTENS KOMMENTAR

"LINK AI er fullstendig isolert fra offentlige systemer. Det er et autonomt verktøy for praktisk hjelp, designet ut fra prinsippet om 'innebygd sikkerhet'."

Beskyttelse mot ekstern tilgang

Lukket distribusjonskrets. Hvorfor applikasjonen ikke kan finnes på nettet utenfra.

-  **Fraværende på offentlige markeder:** Verken i App Store eller Google Play.
-  **Skjult infrastruktur:** Lenken til tjenesten er fysisk utilgjengelig utenfra.
-  **Punktaktivering:** Tilgang gis kun når personen ankommer mottaket.



ARKITEKTENS KOMMENTAR

"Applikasjonen kan ikke lastes ned fra internett. Eksterne personer kan fysisk ikke få tilgang til plattformen – den eksisterer kun innenfor mottakets perimeter."

Tilgang kun via mottakets Wi-Fi

Inngangspunkt – Geofencing. Et digitalt gjerde for å beskytte systemet.

- 1 IP-adressefilter:** Mottar kun forespørsler fra offisielle rutere.
- 2 Aktivering via QR-kode:** Skanning skjer kun på mottakets område.
- 3 Automatisk blokkering:** Systemet deaktiveres når man forlater området.



ARKITEKTENS KOMMENTAR

"Tilgangen er bundet til IP-adressen til mottakets Wi-Fi. Går du utenfor porten, blokkeres systemet. Dette forhindrer misbruk utenfor mottaket."

Prinsippet: "Ingen data – ingen datalekkasje"

Nivå 1 – Arkitektonisk. Absolutt brukeranonymitet.

- ✓ **Uten registrering:** Ingen brukernavn eller passord.
- ✓ **Uten personlige dokumenter:** Krever ikke navn, telefonnummer eller DUF-nummer.
- ✓ **Uten sporing:** Ingen tilgang til enhetens plassering eller kamera.



ARKITEKTENS KOMMENTAR

"Den beste måten å beskytte data på er å ikke samle dem inn. For systemet er hver bruker en anonym gjest. Det finnes ingen data i systemet, så de kan ikke steles."

Plugin-filter for personopplysninger

Nivå 2 – Programvare. Beskytter brukeren mot egne feil.



Avskjæring i sanntid

Kontroll av teksten FØR forespørselen sendes til det nevrale nettverket.



Smart skanning

Umiddelbar gjenkjenning av navn og saksnumre (DUF).



Øyeblikkelig blokkering

Rensing av meldingen på brøkdelen av et sekund uten å lagre logger.

ARKITEKTENS KOMMENTAR

"Jeg har implementert et programvareskjold. Hvis en person i en stresset situasjon tilfeldigvis skriver sitt DUF-nummer, vil skriptet fjerne disse dataene før de når den kunstige intelligensen (KI)."

Mekanikken bak plugin-filteret

Visualisering av datafiltreringsalgoritmen i sanntid.

Blokk INNGANG:

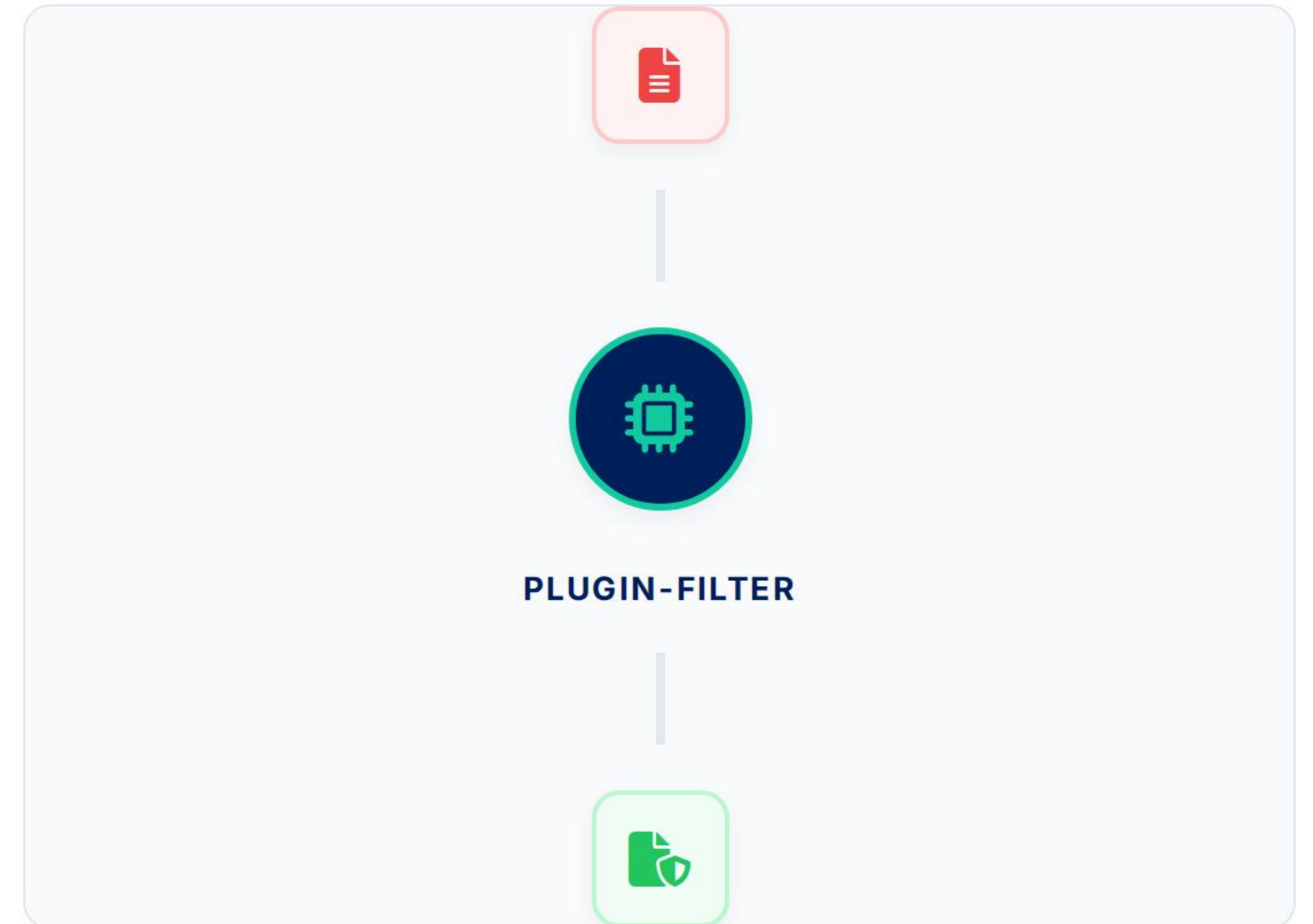
"Jeg er Alex, mitt DUF-nummer er 12345678901, hvor kan jeg hente sengetøy?"



Egendefinert plugin: Fjerning av personopplysninger

Blokk UTGANG:

"Jeg er [Bruker], mitt nummer er [Skjult], hvor kan jeg hente sengetøy?"



ARKITEKTENS KOMMENTAR

"Algoritmen gjør personlige data om til anonymiserte tagger. KI-en ser kun kjernen i spørsmålet (sengetøy), noe som er 100 % i samsvar med GDPR-kravene."

Kommersielt API på bedriftsnivå

Nivå 3 – Juridisk. Lukket krets for databehandling.



Isolert kommunikasjonskanal

Infrastrukturen er bygget på sikker Microsoft Azure.



Offisiell avtale

Signert DPA (Data Processing Agreement) mellom Microsoft og Link AS.



Forbud mot maskinlæring

Dataene er kryptert og mater ikke offentlige KI-modeller fra OpenAI.

ARKITEKTENS KOMMENTAR

"Vi bruker ikke offentlige chat-boter. Arbeidet skjer gjennom en lukket kommersiell krets hos Microsoft, og dataene er juridisk beskyttet mot tredjepartsbruk."

Sertifiserte norske leverandører

Datalokalisering. Fysisk lagring av data innenfor EU/Norge.

- ✓ **Frihet til å velge hosting:** Integrasjon med enhver sertifisert leverandør i Norge.
- ✓ **Juridisk samsvar:** Garanterte dokumenter om datakonfidensialitet og GDPR-samsvar.
- ✓ **Full oppfølging:** Teknisk integrasjon under streng kontroll av Link AS sine jurister.



Data hosted in Norway

ARKITEKTENS KOMMENTAR

"Jeg er helt fleksibel når det gjelder valg av infrastruktur. Servere og lagring vil være strengt plassert i norsk jurisdiksjon under kontroll av deres selskap."

Kontroll over systemplassering

Nivå 4 – Infrastruktur. Tre integrasjonsalternativer tilpasset IT-avdelingens standarder.

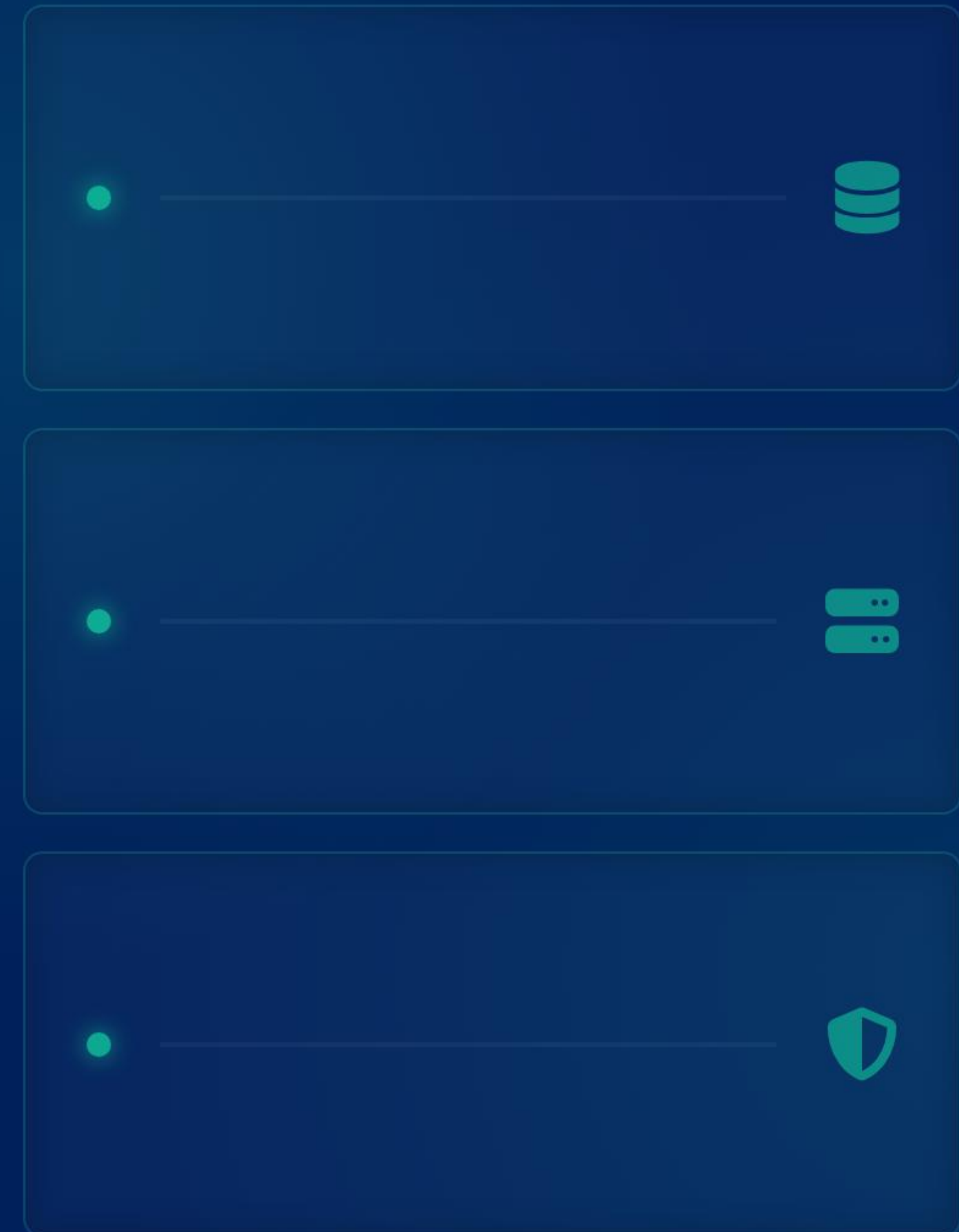
 **Demomodus:** Nåværende status for plattformen for testing.

 **Alternativ A:** Sikker sky i Norge (SSL/TLS-protokoller).

 **Alternativ B:** Lokal server (On-Premises) – full isolasjon innenfor Link AS sin perimeter.

ARKITEKTENS KOMMENTAR

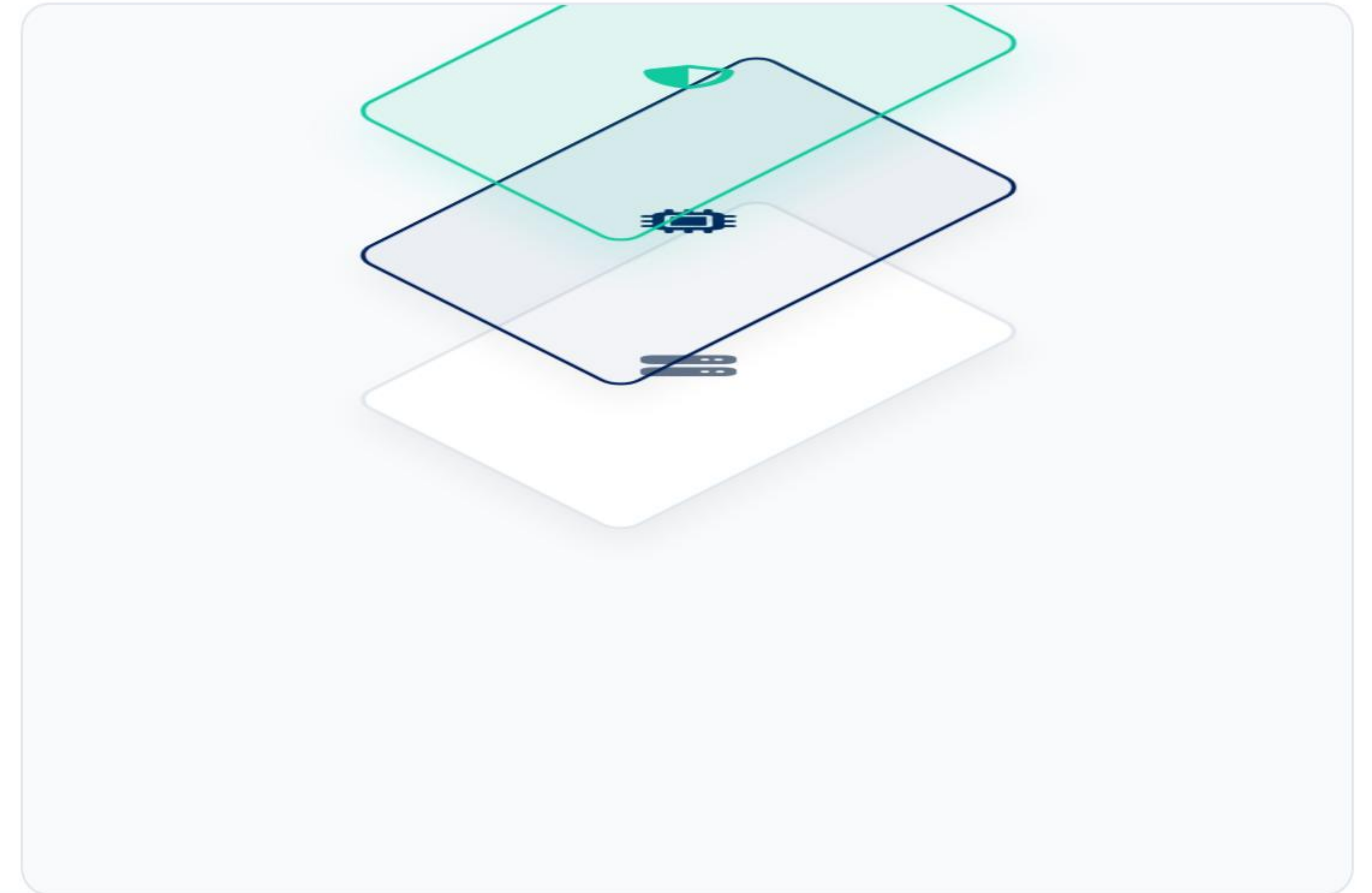
"Jeg gir IT-spesialistene full valgfrihet. Vi kan flytte prosjektet til deres interne servere, og da vil dataene aldri forlate Link AS sitt domene."



Sikkerhetens evolusjon

Arkitektonisk byggesett. Progressiv skalering av beskyttelsen.

-  **Grunnleggende MVP:** 4 sikkerhetsnivåer er tilstrekkelig for trygg og anonym hjelp.
-  **Modulær arkitektur:** Systemet settes sammen som et sikkert IT-byggesett.
-  **Parallell utvikling:** Styrking av sikkerheten synkront med nye funksjoner.



ARKITEKTENS KOMMENTAR

"Prosjektet er et byggesett. Ved introduksjon av nye funksjoner (f.eks. personlige brukerveier) vil sikkerhetsprotokoller utvikles parallelt og kontrolleres av deres IT-avdeling."