# Hvordan vi bruker AI — og hva det betyr for dataene dine

*Et ærlig og tydelig svar til de som skal godkjenne løsningen*

Alle AI-leverandører hevder at produktet deres er sikkert og ivaretar personvernet. Nesten ingen forteller deg hvilken modell-leverandør som faktisk behandler dataene dine, i hvilket land det skjer, under hvilken avtale, eller hva som skjer med dem i etterkant.

Dette er spørsmålene sikkerhets- og personvernteamet ditt vil stille. Dette dokumentet gir svarene for AidEun og SalesQuote.

## Hva vi faktisk bruker AI til

Våre produkter bruker AI til et avgrenset sett med spesifikke oppgaver, ikke som et generelt orakel:

**Svare på spørsmål basert på eget innhold.** AidEun henter relevante dokumenter, tilbud, historiske deler og kunnskapsbaseoppføringer fra dine egne data, og ber en språkmodell formulere svar basert utelukkende på dette materialet. Modellen blir ikke spurt om hva den generelt «vet» — den blir spurt om hva dokumentene dine faktisk sier.

**Lese og strukturere dokumenter.** SalesQuote henter ut ordrelinjer, mengder og spesifikasjoner fra forespørselsdokumenter (RFQ) og e-poster, slik at en person slipper å punche dette manuelt.

**Utarbeide utkast.** Tilbud, svar og sammendrag lages alltid som et utkast som et menneske må gå gjennom — aldri som et endelig svar som sendes ut på vegne av deg uten et menneske i loopen («human-in-the-loop»).

**Søk og gjenfinning.** Vektorer (embeddings) gjør eget innhold søkbart basert på semantisk betydning fremfor bare eksakte nøkkelord.

> **Hva vi ikke gjør:**
> Vi bruker ikke AI til å ta automatiserte beslutninger om personer, vi profilerer ikke kundene dine, og vi bruker aldri dataene dine til å bygge eller trene noe vi selger til andre.

## Hvor AI-prosesseringen faktisk foregår

Dette er spørsmålet de fleste leverandører svarer unnvikende på. Vårt svar er helt konkret:

**Inferens kjøres på Azure OpenAI i Microsofts region Norway East.** Ikke via et delt, offentlig API-endepunkt — men en dedikert Azure OpenAI-ressurs i vårt eget Azure-miljø i Norge. Dette er underlagt Microsofts Data Processing Agreement og dekkes av Microsofts «EU Data Boundary»-forpliktelser.

Dette betyr at spørringene dine (prompts), dokumentene dine og modellens svar forblir innenfor EØS-området. Det skjer ingen overføring til amerikanske leverandører under normal drift av produktet.

**Dataene dine lagres på samme sted.** Databaser, søkeindekser, fillagring og applikasjonstjenester — alt kjører i Microsoft Azure, Norway East. Sikkerhetskopier forblir også innenfor samme region.

**Ingen modeller med kinesisk opprinnelse.** Ingen DeepSeek, ingen Qwen, ingen Kimi — verken i produksjon eller til evaluering.

**Modellvalg er bevisst, ikke tilfeldig.** Plattformen vår er modell-agnostisk av design: et adapterlag gjør at vi kan velge leverandør fremfor å låse dataene dine til én bestemt jurisdiksjon og veikart. Mistral, driftet i Frankrike, er tilgjengelig for kunder som ønsker et spesifikt, europeisk alternativ.

## «Blir dataene våre brukt til å trene andres modeller?»

Nei — og begrunnelsen er viktigere enn selve svaret.

Fellen mange kjøpere går i, handler ikke om hva en leverandør lover muntlig, men hvilket tjenestenivå hos underleverandøren som faktisk benyttes. På gratistjenester hos enkelte leverandører brukes innsendt innhold til å forbedre modellene deres. På betalte enterprise-nivåer gjør det ikke det. Samme modell, samme ledetekst, men en helt annen avtale — og som kunde er det ofte umulig å se hva som foregår bak kulissene.

Å kjøre gjennom Azure OpenAI løser dette strukturelt fremfor gjennom vage løfter. Microsofts vilkår for Azure OpenAI er krystallklare: Dine ledetekster og genererte svar er ikke tilgjengelige for andre kunder, ikke tilgjengelige for OpenAI, og brukes ikke til å trene eller forbedre verken Microsofts eller tredjeparters modeller.

Vår egen databehandleravtale (DPA) gir deg den samme forpliktelsen direkte, slik at dette er et kontraktsfestet ansvar vi har overfor deg, ikke bare et vilkår vi har arvet videre.

## «Kan den hallusinere? Kan den manipuleres?»

Begge deler er reelle risikoer. Enhver leverandør som påstår full immunitet, overselger.

**Om hallusinasjon.** Vår assistent svarer basert på innhentet innhold — dine egne dokumenter som mates inn i modellen som kontekst. Dette er det viktigste strukturelle forsvaret: Modellen blir bedt om å svare ut fra materialet den har foran seg, fremfor fra fri hukommelse. Dette gjør svarene skreddersydd for din virksomhet, og det gjør dem etterprøvbare fordi kilden er umiddelbart tilgjengelig.

Det er likevel ikke et vanntett forsvar. En forankret modell kan fremdeles mistolke et dokument eller påstå noe en kilde ikke fullt ut underbygger. Derfor designer vi løsningen for menneskelig kontroll fremfor full autonomi: AI-leveransen er et utkast som en person må godkjenne, redigere eller avvise. For alt med kommersiell eller kontraktsmessig betydning — som et tilbud eller et kundesvar — er det et menneske i loopen av design, ikke bare som en retningslinje.

**Om «prompt injection» og manipulering.** Dette er ikke et ferdig løst problem i bransjen, og vi vil ikke påstå noe annet. Det mest relevante spørsmålet er ikke «kan den bli lurt», men «hva kan den få tilgang til dersom den blir det». Vårt svar er arkitektonisk: streng isolasjon mellom leietakere (tenants) slik at én kundes data aldri er tilgjengelig fra en annens økt; begrensede rettigheter slik at assistenten kun har tilgang til det den innloggede brukeren uansett har tilgang til; samt menneskelig godkjenning før noe forlater systemet.

Vi jobber kontinuerlig med å herde verktøykjøringsløpet — inkludert validering av input, tillatelseslister for verktøy og verifisering av utdata — som et fast sikkerhetsprogram heller enn en engangsjobb.

## Den usexy delen: Grunnleggende datastyring

Det meste som gjør AI trygt i produksjon, handler ikke om selve AI-teknologien. Det handler om å vite hva man har, hvor lenge det oppbevares, hvem som har tilgang, og å kunne dokumentere det.

**Vi har full kontroll på lagringstider.** Vår slette- og oppbevaringsplan dekker alle enheter i plattformen som inneholder personopplysninger — samtaler, vedlegg, tilbud, logger, embeddings og hurtigbuffere — med fastsatt tidsrom, behandlingsgrunnlag og slettemetode for hver enkelt. Den er godkjent og signert av personvernansvarlig, ledelsen og sikkerhetsansvarlig. Dette er ikke bare en generell erklæring; det er en strukturert oversikt som definerer hva som må slettes sammen med hver oppføring, helt ned til avledede embeddings og mellomlagrede kopier.

**Du kan konfigurere oppbevaringstid selv.** Samtaler kan settes fra 30 dager til 24 måneder, og RFQ-data til 12, 24 eller 36 måneder. Det finnes en nedre grense fordi for kort tid ødelegger arbeidsflyten og kan slette data du trenger, og en øvre grense fordi lagringsbegrensning er et lovpålagt prinsipp. Eventuelle avvik utenfor disse intervallene krever en dokumentert beslutning.

**Sletting betyr fullstendig sletting.** Når en oppføring når slutten av lagringstiden, eller når du ber oss om å slette en registrert persons data, spesifiserer planen hva som fjernes: databaseraden, filobjektet (blob), versjoner og øyeblikksbilder, uthentet innhold, embeddings, forhåndsvisninger og cachede kopier. En embedding overlever aldri kildedokumentet sitt.

**Vårt styringssystem for informasjonssikkerhet er fullt dokumentert.** Vi følger kravene i ISO/IEC 27001:2022: omfang, policyer, risikovurdering, en Statement of Applicability (SoA) som dekker alle 93 Annex A-kontroller, samt ledelsessystemets klausuler for drift, evaluering og forbedring. Interne revisjoner og ledelsens gjennomgang er fast planlagt og ansvarsbelagt.

*Vi er per i dag ikke sertifisert. Vi jobber aktivt mot det, vi vet nøyaktig hvilke kontroller som er åpne, og vi viser deg heller en ærlig gapanalyse enn et sertifikat vi ennå ikke innehar.*

## Hvorfor vi også forteller om det som ikke er ferdig

Fordi du vil oppdage det uansett, og fordi en leverandør som bare ramser opp glansbilder ikke gir deg et reelt beslutningsgrunnlag.

Hver påstand i dette dokumentet er underbygget av styringsdokumenter med versjonsnummer, eier og signatur — eller så er det tydelig beskrevet som pågående arbeid. Avvik og funn følges opp som oppgaver med datoer og navngitte ansvarlige. Våre underdatabehandlere, lokasjoner og overføringsmekanismer er offentlig tilgjengelige på aisolutions.no/suppliers. Vår databehandleravtale (DPA) er tilgjengelig på aisolutions.no/dpa.

Dersom sikkerhets- eller personvernteamet ditt ønsker å gå grundigere til verks — innsyn i sletteplanen, gapanalysen eller overføringsvurderinger — er det bare å ta kontakt. Vi tar den samtalen langt heller i innkjøpsfasen enn etter en hendelse.

**Spørsmål:** thore@aisolutions.no
*AISolutions AS · Org. nr 931 884 220 · Spannavegen 152, 5535 Haugesund, Norge*