

AI-sikkerhed – en løsning i kundens egen AI

Human Intel OÜ / AI for Logistics

Vores tilgang er designet til at give kunden en specialiseret salgs-AI uden, at vi behøver at installere software i eller arbejde direkte i virksomhedens øvrige IT-systemer.

Kort fortalt: Vi konfigurerer salgs-AI'en direkte i kundens egen valgte AI-plattform – fx ChatGPT, Claude, Gemini, Mistral eller en anden understøttet AI-plattform. Kunden beholder dermed sin egen konto, sine egne brugerrettigheder og sin egen kontrol over AI-miljøet.

Vi arbejder ikke inde i kundens IT-infrastruktur

- Standardleverancen kræver ikke, at Human Intel OÜ eller NexusValue.ai får adgang til kundens ERP-system, CRM, økonomisystem, filserver, Microsoft 365-miljø, Google Workspace eller øvrige interne systemer.
- Opsætningen sker i kundens egen AI-konto eller workspace. Det betyder, at kunden selv vælger AI-udbyder, abonnementsstype, brugere, adgangsrettigheder og hvilke oplysninger der må lægges ind i AI'en.
- Hvis kunden senere ønsker integrationer til fx CRM, dokumentbiblioteker eller andre datakilder, er det en særskilt beslutning. Sådanne integrationer aktiveres ikke automatisk som en del af standardopsætningen.

Sikkerheden følger kundens valgte AI-plattform

Den tekniske behandling af prompts, filer og AI-svar sker hos den AI-udbyder, kunden selv har valgt. Derfor afhænger den konkrete sikkerhed, datalagring og administration også af kundens abonnement og indstillinger hos den pågældende udbyder.

Platform	Eksempler på virksomhedsbeskyttelse
ChatGPT Business / Enterprise	OpenAI oplyser, at virksomhedsdata som standard ikke bruges til modeltræning. Data krypteres i hvile med AES-256 og under transport med TLS 1.2 eller nyere. Enterprise-funktioner omfatter bl.a. adgangsstyring og compliance-kontroller.
Claude Enterprise	Anthropic oplyser, at inputs og outputs fra Enterprise-konti ikke bruges til træning. Enterprise tilbyder bl.a. SSO, SCIM, rollebaseret adgang, audit-/compliance-funktioner og tilpassede retention-indstillinger.
Google Workspace med Gemini	Google oplyser, at Workspace-data ikke bruges til at træne de underliggende generative AI-modeller uden kundens tilladelse. Eksisterende Workspace-kontroller som adgangsrettigheder, DLP og dataregioner kan fortsat anvendes.
Mistral Team / Enterprise	Mistral oplyser, at input og output på Team- og Enterprise-planer ikke bruges til modeltræning. Mistral tilbyder desuden privacy- og data controls, GDPR-rettigheder og relevante muligheder for bl.a. zero data retention afhængigt af produkt og endpoint.

Kunden bevarer kontrollen

- Kunden ejer og administrerer sin AI-konto og bestemmer, hvem der har adgang.
- Kunden kan selv fastlægge interne regler for, hvilke data medarbejdere må bruge i AI'en.
- Vi anbefaler virksomhedsversioner af AI-plattformene frem for private/gratis konti, når løsningen bruges professionelt.

- NexusValue.ai's koncept, metoder, prompts, instruktioner, agentopsætninger og øvrige materiale om Værdifokuseret Salg leveres som en brugsret under det aktive abonnement og forbliver NexusValue.ai's immaterielle rettigheder.
- Når aftalen ophører, skal NexusValue.ai-materialet fjernes fra kundens AI-miljø i henhold til serviceaftalen.

Hvad kunden stadig selv skal tage stilling til

Ingen AI-løsning er "automatisk sikker" alene fordi den ligger hos en stor AI-udbyder. Kunden bør vælge en passende business/enterprise-plan, konfigurere adgang korrekt og følge egne informationssikkerhedsregler. Særligt følsomme oplysninger, persondata, forretningshemmeligheder eller regulatorisk beskyttede data bør kun anvendes, hvis kundens egne politikker og den valgte AI-plattform tillader det.

Vores sikkerhedsprincip

Mindst mulig adgang. Mest mulig kundekontrol. Vi bygger salgs-AI'en dér, hvor kunden allerede har valgt at arbejde med AI. Standardløsningen kræver derfor ikke, at vi får en teknisk "bagdør" ind i kundens øvrige IT-miljø. Det reducerer integrationsfladen og gør ansvarsfordelingen mere overskuelig: kunden styrer AI-kontoen og sine data, AI-udbyderen står for den tekniske platform, og Human Intel OÜ/NexusValue.ai står for opsætning, træning, vedligeholdelse og den værdifokuserede salgsmetodik.

Kilder og dokumentation

- OpenAI – Business data privacy, security and compliance: [OpenAI - Business data privacy](#)
- OpenAI – Enterprise privacy: [OpenAI - Enterprise privacy](#)
- Anthropic – Enterprise security / CIO & IT guidance: [Anthropic - Enterprise security](#)

Google Workspace – Generative AI security, compliance and privacy: [Google Workspace: AI-privatliv og sikkerhed \(officiel kilde\)](#)

Mistral AI – Privacy and data controls: [Mistral: Privacy & Data Controls \(officiel dokumentation\)](#)

Mistral AI – Data training controls: [Mistral: Brug af kundedata til modeltræning \(officiel hjælp\)](#)

Bemærkning: Sikkerhedsfunktioner varierer efter AI-udbyder, abonnementstype og kundens egne indstillinger. Denne tekst er en generel beskrivelse af leverancemodellen og erstatter ikke kundens egen IT-sikkerheds- eller compliance-vurdering.

Vigtig disclaimer

Dette dokument er generel information om AI for Logistics' leverancemodell og om de nævnte AI-platfomes offentligt beskrevne sikkerhedsfunktioner. Det er ikke juridisk rådgivning, en sikkerhedscertificering eller en garanti for en bestemt platform, konfiguration eller kundes compliance-status. Funktioner, vilkår, databehandling og sikkerhedsindstillinger kan ændres hos tredjepartsudbydere. Kunden er derfor ansvarlig for egen risikovurdering, valg og konfiguration af AI-plattform, dataklassifikation, adgangsstyring samt overholdelse af egne politikker og gældende lov- og myndighedskrav.