

Alamigo AI-politik

Rammer for ansvarlig, sikker og dokumenterbar anvendelse af kunstig intelligens

Dokument	Oplysning
Dokumentejer	Alamigos ledelse
Version	1.2
Gældende fra	23. august 2026
Klassifikation	Offentlig - gratis eksempel
Næste gennemgang	Senest 23. august 2027 eller ved væsentlige ændringer

Grundprincip: AI kan understøtte arbejdet, men mennesker har altid det endelige ansvar for beslutninger, kvalitet og offentliggjort indhold.

Gratis eksempel: Dokumentet må frit downloades, anvendes og tilpasses. Kildeangivelse er velkommen, men ikke et krav. Det er generel information og ikke juridisk rådgivning.

Formål og anvendelsesområde

Politikken fastlægger Alamigos fælles rammer for ansvarlig, sikker og hensigtsmæssig anvendelse af AI. Den skal samtidig understøtte efterlevelse af EU's AI-forordning, databeskyttelsesregler og anden relevant lovgivning.

Politikken gælder for medarbejdere, ledelse, konsulenter og samarbejdspartnere, der anvender AI-systemer under Alamigos ansvar eller på Alamigos vegne. Privat brug uden forbindelse til arbejdet er ikke omfattet.

1. Principper for anvendelse af AI

- **Ansvar:** Et menneske træffer og ejer den endelige beslutning.
- **Kvalitet:** AI-output kontrolleres i forhold til opgavens betydning og risiko.
- **Gennemsigtighed:** AI-brug oplyses, når det er relevant eller krævet.
- **Datasikkerhed:** Kundeoplysninger, personoplysninger og interne informationer beskyttes.
- **Fairness:** AI må ikke anvendes diskriminerende, manipulerende eller på anden måde uforsvarligt.
- **Dokumentation:** Væsentlige anvendelser og kontroller skal kunne forklares efterfølgende.

2. Tilladte, begrænsede og forbudte anvendelser

AI må blandt andet anvendes til research, analyse, idéudvikling, tekstudkast, programmering, oversættelse, præsentationer, billeder, video og automatisering, når brugen følger denne politik.

AI må ikke stå alene som beslutningsgrundlag ved juridiske, økonomiske, personalemæssige, sikkerhedsmæssige eller strategiske vurderinger. Kontrol, dokumentation og godkendelse skal øges, når konsekvensen af fejl er større.

2.1 Anvendelser, der kræver særskilt godkendelse

Før følgende anvendelser påbegyndes, skal ledelsen eller den AI-ansvarlige funktion dokumentere formål, datagrundlag, risici, menneskelig kontrol og relevante juridiske krav:

- beslutningsstøtte, der kan få væsentlig betydning for ansættelse, adgang til ydelser, økonomi, sundhed, jura eller sikkerhed
- biometrisk kategorisering, følelsesgenkendelse, medarbejdermonitorering eller anden systematisk vurdering af personer
- automatiseret publicering eller eksterne handlinger i større omfang, hvor fejl kan påvirke mange mennesker eller kunder
- behandling af større mængder fortrolige, følsomme eller forretningskritiske data
- udvikling eller udbud af et AI-system under Alamigos eget navn eller varemærke.

2.2 Forbudte anvendelser

AI må ikke anvendes til:

- manipulerende eller vildledende metoder, der kan skade mennesker eller væsentligt svække deres mulighed for at træffe en informeret beslutning
- diskrimination, ulovlig profilering, social scoring eller skjult og uberettiget overvågning
- skjult efterligning, falske udsagn, falske kundeudtalelser eller fremstillinger, der tillægger personer handlinger, som ikke er reelle
- fuldautomatiske afgørelser med væsentlig betydning for personer uden passende menneskelig vurdering og mulighed for indgriben
- behandling af adgangskoder, tokens, ulovligt indsamlede data eller andre oplysninger, som ikke må behandles i den konkrete løsning.

3. Godkendte AI-værktøjer

Alamigo Browser AI er virksomhedens primære AI-plattform. Andre AI-værktøjer må kun anvendes, når de er godkendt af ledelsen eller indgår som en godkendt del af Alamigos platform og arbejdsgange.

En godkendelse skal som minimum tage stilling til anvendelsesformål, datatyper, adgangsforhold, leverandørvilkår, opbevaring og eventuel brug af data til træning.

Ledelsen vedligeholder et værktøjsregister med systemejer, tilladte formål og datakategorier, adgangsforhold, opbevaring, leverandørens brug af data, seneste godkendelsesdato og eventuelle begrænsninger.

Brugeren skal kontrollere værktøjsregistret og de konkrete instruktioner, før et nyt værktøj, en ny funktion eller en ny datatype anvendes.

4. Data- og informationssikkerhed

Følgende må ikke indtastes i et ikke-godkendt AI-system:

- følsomme eller fortrolige personoplysninger
- fortrolige kundeoplysninger eller materiale omfattet af tavshedspligt
- forretningshemmeligheder eller ikke-offentliggjort strategisk information
- adgangskoder, API-nøgler, tokens eller andre legitimationsoplysninger
- kildekode eller sikkerhedsoplysninger, som ikke er godkendt til den konkrete løsning.

Oplysninger må kun behandles i en AI-løsning, når datatypen og anvendelsen er godkendt, og relevante kontraktuelle, organisatoriske og tekniske sikkerhedsforanstaltninger er på plads.

4.1 Logning, opbevaring og adgang

Prompts, output, logdata og vedhæftede filer må kun opbevares til et sagligt og dokumenteret formål og ikke længere end nødvendigt. Adgang gives efter arbejdsbetinget behov og gennemgås regelmæssigt.

Når en person fratræder, et projekt afsluttes eller et værktøj ikke længere er godkendt, fjernes adgangen, og data slettes, eksporteres eller arkiveres efter den gældende opbevaringsregel.

5. Kvalitet og menneskelig kontrol

Den ansvarlige bruger skal vurdere AI-output kritisk og kontrollere væsentlige oplysninger mod troværdige kilder. AI må ikke betragtes som en autoritativ faktakilde.

Ved offentliggørelse om forhold af offentlig interesse skal den menneskelige kontrol være indholdsmæssig. Den omfatter efter behov faktatjek, kildekontrol og en reel mulighed for at ændre eller afvise teksten. Ren stave- eller grammatikkontrol er ikke tilstrækkelig som redaktionel kontrol.

6. Gennemsigtighed og eksternt indhold

Alamigos AI-indholdspolitik fastlægger de operationelle regler for tekst, billeder, video, sociale medier, hjemmeside og chatbots. Følgende minimumskrav gælder:

- Brugere skal klart, skelneligt og tilgængeligt fra første interaktion kunne forstå, når de kommunikerer direkte med en AI-assistent, medmindre det er helt åbenlyst.

- Deepfakes og andet omfattende syntetisk indhold mærkes klart, skelneligt og tilgængeligt senest ved første eksponering, når reglerne kræver det.
- Hvis Alamigo anvender følelsesgenkendelse eller biometrisk kategorisering, skal anvendelsen være særskilt godkendt, og berørte personer skal informeres før behandlingen, når reglerne kræver det.
- Maskinlæsbar mærkning eller metadata må ikke fjernes uden en dokumenteret, saglig grund.
- Offentligt indhold har en identificerbar person eller funktion med redaktionelt ansvar.

7. Roller og ansvar

Ledelsen

- godkender politikken, væsentlige AI-anvendelser og tilladte værktøjer
- fastlægger passende kontrol- og kompetenceniveauer
- sikrer, at hændelser og væsentlige afvigelser bliver håndteret.

AI-ansvarlig funktion

- vedligeholder værktøjs- og anvendelsesregisteret og koordinerer risikovurderinger
- følger op på AI-færdigheder, dokumentation, hændelser og væsentlige ændringer i regler eller værktøjer
- kan varetages af ledelsen, indtil en særskilt ansvarlig er udpeget.

Brugere af AI

- følger denne politik og de konkrete instruktioner for værktøjet
- beskytter data og kontrollerer output før anvendelse eller offentliggørelse
- beder om hjælp eller stopper anvendelsen ved tvivl
- rapporterer fejl, sikkerhedshændelser og væsentlige risici.

8. AI-færdigheder

AI-færdigheder: Alamigo skal ikke blot forvente, at medarbejdere kan anvende AI. Virksomheden skal aktivt sikre og kunne dokumentere et tilstrækkeligt niveau af AI-færdigheder.

Alamigo fastlægger det nødvendige kompetenceniveau ud fra personens rolle, tekniske viden og erfaring, det anvendte AI-system, anvendelseskonteksten samt de personer eller grupper, som anvendelsen kan påvirke.

8.1 Introduktion før eller ved ibrugtagning

Personer, der bruger AI på Alamigos vegne, skal modtage en relevant introduktion. Den tilpasses rollen og omfatter som minimum:

- hvilke AI-værktøjer og anvendelser der er godkendt, og hvilke data der må og ikke må anvendes
- kendte begrænsninger, herunder fejl, hallucinationer og bias, samt krav til faktatjek, kvalitetssikring og menneskeligt ansvar
- regler om ophavsret, fortrolighed og personoplysninger
- krav om gennemsigtighed og mærkning, hvor det er relevant
- hvordan tvivl, fejl og hændelser rapporteres.

8.2 Løbende vedligeholdelse

AI-færdigheder vedligeholdes løbende og revurderes mindst én gang årligt samt ved væsentlige ændringer i værktøjer, anvendelser, risici eller lovgivning. Eksisterende erfaring og uddannelse kan indgå i vurderingen; supplerende oplæring gives efter behov.

8.3 Dokumentation

Alamigo dokumenterer kompetenceindsatsen i et omfang, der er passende for virksomhedens størrelse og AI-anvendelse. Dokumentationen kan være enkel og skal som minimum vise:

- dato og målgruppe
- hvilket materiale eller hvilke emner der blev gennemgået
- hvem der gennemførte eller kvitterede for introduktionen
- eventuelle rollebaserede eller systembaserede tillæg
- dato for næste vurdering eller opdatering.

En e-mailkvittering, en kort træningslog eller registrering i virksomhedens dokumentationssystem kan anvendes, hvis indhold og gennemførelse kan dokumenteres.

9. Hændelser, tvivl og afvigelser

Brugeren skal straks standse eller begrænse anvendelsen og rapportere til ledelsen via Alamigos interne sikkerhedskanal, hvis et AI-system giver anledning til mistanke om dataleak, væsentligt urigtigt eller diskriminerende output, ulovlig anvendelse, vildledning eller anden betydelig risiko.

Væsentlige hændelser dokumenteres med dato, system, hændelsesbeskrivelse, berørte data eller personer, foretagne handlinger og beslutning om videre brug.

Ledelsen udpeger en hændelsesejer, begrænser skaden, sikrer relevante logs og beviser og vurderer behovet for at informere kunder, berørte personer, rådgivere eller myndigheder. Anvendelsen genoptages først, når risikoen er accepteret eller afhjulpet.

Mistanke om brud på persondatasikkerheden håndteres straks efter Alamigos almindelige beredskab og de gældende GDPR-frister.

10. Compliance

Alamigo anvender AI i overensstemmelse med relevant lovgivning og virksomhedens øvrige politikker, herunder EU's AI-forordning, GDPR, markedsføringsloven og ophavsretsreglerne. Politikken indebærer ikke i sig selv, at enhver konkret anvendelse er lovlig; den enkelte brugssituation skal vurderes efter behov.

Undtagelser fra politikken kræver en forudgående, dokumenteret godkendelse fra ledelsen med begrundelse, risikovurdering, varighed og kompenserende kontroller.

Overtrædelser kan medføre begrænset adgang, korrigerende oplæring og andre proportionale tiltag. Alvorlige eller gentagne overtrædelser eskaleres til ledelsen.

11. Revision og ikrafttræden

Version 1.2 træder i kraft den 23. august 2026. Ledelsen gennemgår den mindst én gang årligt og tidligere ved væsentlige ændringer i lovgivning, teknologi, Alamigos produkter eller anvendelsesmønstre.

Versionshistorik

Version	Dato	Ændring	Godkendelse
1.0	Juli 2026	Første udgave	Ledelsen
1.1	03.08.2026	AI-færdigheder, dokumentation og præcisering af gennemsigtighed	Ledelsen
1.2	23.08.2026	Offentlig eksempelversion, risikogodkendelser, værktøjsregister, opbevaring og hændelsesproces	Ledelsen

Referencer

- [EU-forordning 2024/1689 om kunstig intelligens](#)
- [Digitaliseringsstyrelsen: AI-færdigheder](#)
- [EU-Kommissionen: Gennemsigtighedsforpligtelser efter artikel 50](#)

Alamigos princip: Vi bruger AI til at skabe større værdi for mennesker - aldrig til at flytte ansvaret fra mennesker.