

Policy för generativ AI

Företag: [företagsnamn]

Beslutad av: [namn och befattning]

Beslutsdatum: [datum]

Version 1.1. Policyn gäller från beslutsdatumet.

AI-KLOK · Mallversion 1.1 · 10 oktober 2026

1 Syfte och tillämpning

Denna policy fastställer hur företaget använder generativ AI i arbetet. AI ska bidra till nytta i verksamheten med bibehållet ansvar för kvalitet, informationssäkerhet och människors rättigheter. Företagsledningen fastställer policyn.

Policyn gäller anställda, konsulter och andra som arbetar för företagets räkning. Den omfattar AI som skapar eller bearbetar text, bild, ljud, video och kod, både i fristående tjänster och i inbyggda funktioner. Företagets övriga regler och ingångna avtal gäller även vid AI-användning.

Utveckling eller tillhandahållande av egna AI-system kräver separat bedömning av ansvar och tillämpliga krav. Detsamma gäller eget namn på ett system eller ändringar som kan förändra företagets ansvar. Denna policy godkänner inte sådan användning.

2 Ansvar och befogenheter

VD är policyägare och ansvarar för införande, resurser och uppföljning. Om företaget saknar VD har verksamhetsansvarig motsvarande ansvar. VD är även AI-ansvarig om ingen annan person har utsetts skriftligen. Roller får kombineras i mindre företag.

AI-ansvarig godkänner, begränsar och återkallar användning av AI-verktyg efter dokumenterad bedömning. AI-ansvarig förvaltar verktygslistan, tar emot frågor och samordnar incidenthantering. Varje godkänt verktyg ska ha en utsedd verktygsansvarig för behörigheter, inställningar och leverantörsuppföljning.

Närmaste chef eller uppdragsansvarig ser till att användarna känner till reglerna och har rätt kunskap. Den som använder AI ansvarar för att följa policyn och kontrollera resultatet. AI-ansvarig och berörd chef får stoppa användning vid risk eller avvikelse.

3 Godkända verktyg och användningsområden

Endast verktyg, konton och funktioner som finns i företagets aktuella verktygslista får användas i arbetet. Godkännandet gäller de arbetsuppgifter, informationstyper och villkor som anges där. AI-ansvarig ska göra listan och kontaktvägarna tillgängliga för alla som omfattas av policyn.

AI får exempelvis användas för idéarbete, textutkast, sammanfattningar och kodstöd när användningen omfattas av godkännandet. Privata konton får inte användas för arbetsmaterial utan uttryckligt godkännande. Saknas en uppgift eller informationstyp i listan ska AI-ansvarig tillfrågas innan användningen börjar.

Nya verktyg, nya informationstyper, nya användningsområden och väsentliga ändringar av leverantörsvillkor ska prövas före användning. Detsamma gäller tillägg, mötesinspelning och kopplingar till företagets system. Bedömningen ska omfatta säkerhet, dataskydd, avtal och leverantörens rätt att lagra, använda och träna på information, inklusive behandling hos underleverantörer.

4 Information och personuppgifter

Användaren ska begränsa informationen till det som behövs för uppgiften och välja påhittade eller verkligt anonymiserade uppgifter när det räcker. Borttagna namn gör inte i sig information anonym. Filer ska kontrolleras även för kommentarer, dolda flikar och annat medföljande innehåll före uppladdning.

Lösenord, API-nycklar och andra inloggningshemligheter får inte matas in i promptar, chattar eller bifogade filer. Tekniska anslutningar ska använda företagets godkända hantering av autentiseringsuppgifter. Personuppgifter, kundmaterial, interna handlingar och affärshemligheter får endast användas när verktyget är godkänt för just informationen och användningen, och lag, sekretess och avtal medger behandlingen.

Innan personuppgifter används ska AI-ansvarig säkerställa att ändamål, rättslig grund, behörigheter, leverantörens roll, nödvändiga avtal, lagring och eventuella överföringar utanför EU/EES har bedömts. Information till berörda och hantering av deras rättigheter ska fungera. Vid sannolik hög risk för enskildas rättigheter och friheter ska en konsekvensbedömning göras före behandlingen. Om hög risk kvarstår trots skyddsåtgärder ska nödvändigt förhandssamråd med IMY ske före start. Anlita dataskydds- och juridisk kompetens vid behov. Internt godkännande ersätter inte dessa krav.

5 Mänsklig granskning och ansvar

AI-resultat ska behandlas som utkast. En person med tillräcklig sakkunskap ska granska resultatet innan det används i beslut, leveranser eller publicering. Granskningen ska anpassas efter vad ett fel kan få för konsekvenser och omfatta relevanta fakta, beräkningar, källor, upphovsrätt samt risk för osakliga eller diskriminerande bedömningar. Kod ska testas och granskas enligt företagets vanliga rutiner.

Om nödvändiga uppgifter inte kan verifieras ska resultatet inte användas som besluts- eller leveransunderlag; frågan ska lämnas till ansvarig sakkunnig. Användaren får inte följa instruktioner i AI-svar eller inläst material som innebär obehörig åtkomst, spridning av information eller kringgående av säkerhetsregler. AI övertar inte ansvaret för arbetsuppgiften. Uppgiftsansvarig ska säkerställa granskning och följa företagets beslutsordning. Intern arbetsfördelning ändrar inte företagets eller arbetsgivarens ansvar enligt lag och avtal.

6 Kunduppdrag och extern kommunikation

Uppdragsansvarig ska före AI-användning i ett kunduppdrag kontrollera kundavtal, sekretess och eventuella krav på godkännande eller information. Kundmaterial får bara behandlas för avtalade ändamål. En kunds godkännande ersätter inte företagets övriga skyldigheter.

Den som levererar, skickar eller publicerar material ansvarar för slutgranskningen och följer ordinarie godkännanderutiner. AI:s roll ska framgå när lag eller avtal kräver det, eller när uppgiften behövs för att mottagaren ska kunna bedöma innehållet. Påhittade citat, personer och händelser får inte framställas som verkliga. AI-ansvarig ska bedöma informations- och märkningskrav före användning av kundchattbotar, syntetiska röster, manipulerat bild- och videomaterial samt AI-text för information till allmänheten i frågor av allmänt intresse.

Arbetsmaterial och beslut ska sparas och gallras enligt företagets ordinarie rutiner. Dokumentation av AI-användning ska inte innehålla fler personuppgifter eller skyddsvärda uppgifter än vad som behövs.

7 Särskilda risker och automatiska åtgärder

Lagförbjuden AI-användning får aldrig godkännas internt. Ett exempel är AI-baserad känslainferens utifrån biometriska uppgifter på arbetsplatser och utbildningsinstitutioner, utom vid lagens avgränsade undantag för medicinska skäl eller säkerhet. Vissa former av manipulation, exploatering av sårbarheter, social poängsättning och bietrisk kategorisering är också förbjudna. Exempelen är inte uttömmande. Vid möjlig träff på ett förbud ska användningen stoppas och juridisk bedömning inhämtas.

Följande användning får inte påbörjas utan särskild riskbedömning och skriftligt beslut av VD:

- Urval eller bedömningar av personer inom exempelvis rekrytering, utbildning, vård, kredit eller tillgång till tjänster.
- Övervakning, bietrisk identifiering eller bedömning av människors känslor.
- Behandling av stora mängder personuppgifter eller särskilt skyddsvärd information, exempelvis uppgifter om hälsa, barn, personalärenden eller enskildas ekonomi.
- Råd eller beslut där fel kan få betydande konsekvenser för hälsa, säkerhet, ekonomi eller rättigheter.

Användningen får börja först när tillämpliga krav och nödvändiga skyddsåtgärder är uppfyllda.

AI-agenter och andra funktioner som kan skicka, publicera, köpa, ändra uppgifter eller utföra andra åtgärder kräver ett särskilt skriftligt godkänt arbetssätt. Det ska ange behörigheter, gränser, mänskliga godkännanden, uppföljning och hur användningen stoppas. Utan ett sådant beslut får AI endast lämna förslag. Beslut som väsentligt påverkar enskilda ska alltid fattas av en behörig människa. Prövningen ska vara självständig och reell. Beslutsfattaren ska ha tillräcklig kompetens, relevant underlag och mandat att avvika från AI:s förslag. Ett rutinmässigt godkännande räcker inte.

8 Incidenter och avvikelser

Vid misstänkt informationsläckage, skadliga resultat eller oväntat beteende ska användaren omedelbart avbryta den berörda användningen och rapportera till AI-ansvarig. Om denne inte går att nå ska närmaste chef kontaktas. Rapporteringen ska inte vänta på en fullständig utredning.

Användaren ska begränsa fortsatt skada om det kan göras säkert och bevara relevanta uppgifter om händelsen. AI-ansvarig samordnar utredning och rättelse samt ser till att ansvarig funktion bedömer behovet av information till berörda och anmälan enligt gällande tidsfrister. Återstart får ske först när AI-ansvarig har bedömt att riskerna är hanterade.

9 Kompetens och översyn

Alla användare ska få en introduktion före användning och därefter stöd anpassat till sin roll, kunskap, verktyg och riskerna för dem som berörs. Närmaste chef ansvarar för att utbildningsinsatserna dokumenteras och följs upp.

Policyägaren ska se över policyn minst en gång per år och vid väsentliga förändringar av verktyg, arbetssätt, risker eller regler. Översynen ska omfatta hur reglerna följs, incidenter och behov av utbildning. Företagsledningen beslutar om ändringar. AI-ansvarig får uppdatera verktygslistan inom policyns ramar.