

Inför företagets policy för generativ AI

Anpassningsguide och verktygsbilaga från AI-KLOK

Om guiden

Guiden hjälper policyägaren att införa grundmallen för generativ AI som arbetsstöd. Medarbetarna får den separata huvudpolicyen. Andra AI-system, egna AI-tjänster och branschkrav behöver ett kompletterande upplägg. Börja med en konkret arbetsuppgift och godkänn bara prövad användning.

Anpassa mallen till verksamheten. Den är inte juridisk rådgivning eller en efterlevnadsgaranti. VD-beslut, verktygslista, årlig översyn och mänsklig beslutspunkt är föreslagna interna regler. Lagkrav gäller när deras förutsättningar är uppfyllda. Ta in relevant kompetens vid personuppgifter, särskilda risker och oklarheter.

1 Anpassa ansvar och kontaktvägar

Fyll i företag, beslutsfattare och beslutsdatum i huvudpolicyen. Kontrollera mandatet. Policyen gäller från beslutsdatumet; ange ett annat startdatum om det behövs. Uppdatera versionen vid ändringar.

VD, eller verksamhetsansvarig om VD saknas, är som standard både policyägare och AI-ansvarig. Utse en annan AI-ansvarig skriftligen vid behov. AI-ansvarig är en intern samordningsroll. Företagets dataskyddsroll och ett eventuellt dataskyddsombuds självständighet kvarstår. Undvik intressekonflikter när roller kombineras.

Gör följande uppgifter tillgängliga för alla användare:

AI-ansvarig och kontaktväg: [namn, e-post eller telefon]

Reservkontakt vid incident: [namn eller funktion och kontaktväg]

Verktygslista och relaterade rutiner: [gemensam plats eller länk]

Koppla policyn till rutiner för informationssäkerhet, dataskydd, inköp, publicering och dokumenthantering. Utse ansvariga för rättighetsbegäranden och personuppgiftsincidenter. Kontaktvägarna ska fungera; en jourfunktion krävs inte generellt. Utan godkända verktyg tillåter policyn ingen AI-användning i arbetet.

2 Pröva arbetsuppgiften och leverantören

Beskriv uppgiften, nyttan, användarna och vilka personer som berörs. Pröva kundavtal, sekretess, upphovsrätt och branschkrav. Dokumentera beslut, begränsningar och underlag. Kontrollerna ska omfatta:

- Leverantör och kontotyp, villkor och användning av indata eller resultat för träning, vidareutveckling eller andra ändamål.
- Information som behövs, behörigheter, säkerhetsinställningar, lagringstid, radering, behandlingsländer, underleverantörer och systemkopplingar.
- Granskning av resultat, incidenter, ändringar och avslut. För agenter behövs åtgärdsgränser, mänskliga godkännanden och en fungerande stoppfunktion.

Bedöm hur AI förändrar arbetsuppgifter, arbetsbelastning och kompetensbehov. Vid planerade verksamhetsändringar ska arbetsmiljöriskerna undersökas, bedömas och dokumenteras. Ge arbetstagare och skyddsombud möjlighet att medverka. Pröva före beslut om information, samverkan eller förhandling krävs enligt lag eller kollektivavtal. Det beror på förändringen och partsförhållandena. Ansvarig chef genomför åtgärderna. Se AFS 2023:1 §§6 och 11 samt MBL §§11-13, källor 7-8.

3 Hantera personuppgifter före start

Pröva varje behandling och ändamål

Dokumentera rättslig grund för den konkreta behandlingen. Vid intresseavvägning ska intresset, nödvändigheten och avvägningen prövas. Kontrollera ytterligare villkor för känsliga personuppgifter och uppgifter om lagöverträdelser enligt GDPR artiklarna 9-10. Hälsa omfattas av artikel 9; uppgifter om barn, ekonomi eller personalärenden gör det inte automatiskt. Bedöm även nya ändamål, exempelvis leverantörsträning. Kodade uppgifter som kan kopplas till en person är inte anonyma. Använd inte en icke godkänd tjänst för att anonymisera skyddade originaluppgifter.

Fastställ roller och avtal

Företagets och leverantörens faktiska behandling avgör dataskyddsrollerna. När leverantören behandlar uppgifter för företagets räkning krävs biträdesavtal enligt artikel 28 och kontroll av underbiträden. Är företaget själv biträde åt en kund, följ kundens instruktioner och kontrollera nödvändigt underbiträdestillstånd. Gemensamt personuppgiftsansvar kräver en bedömning enligt artikel 26. Leverantörens egen användning blir inte tillåten enbart genom ett biträdesavtal.

Kontrollera överföringar och skydd

Kontrollera lagring och åtkomst för mottagare utanför EU/EES, även genom support och underbiträden. Dokumentera stöd enligt GDPR:s kapitel V, exempelvis ett tillämpligt adekvansbeslut eller standardavtalsklausuler med nödvändig bedömning och kompletterande skydd. EU-lagring eller avstängd träning räcker inte i sig. Verifiera beslutade skydd för åtkomst, gallring, återställning och leverantörsinställningar. Uppdatera behandlingsregistret när registreringsskyldighet gäller; verktygslistan ersätter det inte automatiskt.

Ordna information och rättigheter

Säkerställ att berörda får den GDPR-information som krävs. AI-märkning ersätter inte den informationen. Utse ansvarig funktion och dokumentera kontaktväg, tidsfrister och leverantörens medverkan för tillämpliga rättigheter, exempelvis tillgång, rättelse, radering, begränsning och invändning. Omfatta indata, resultat och sparad historik. Alla rättigheter gäller inte ovillkorligt. En begäran ska besvaras utan onödigt dröjsmål och normalt senast en månad efter mottagandet. Vid behov får fristen förlängas med högst två månader till med hänsyn till komplexitet och antal begäranden. Informera om förlängningen och skälen inom den första månaden. Vid avslag ska skäl och information om möjligheten till klagomål och rättslig prövning lämnas enligt artikel 12.4.

Genomför nödvändig konsekvensbedömning

Vid sannolik hög risk för enskildas rättigheter och friheter ska en konsekvensbedömning avseende dataskydd, DPIA, göras innan behandlingen börjar. Kvarstår hög risk trots planerade skydd ska nödvändigt förhandssamråd med IMY ske före start. GDPR:s riskprovning är skild från AI-förordningens högriskklassificering. Ett VD-beslut ersätter ingen av dem. Se GDPR artiklarna 5-6, 9-22, 26, 28, 30, 32, 35-36, 38 och 44-49 samt IMY, källor 3-4.

4 Pröva lagkraven för AI

Kontrollera förbud och företags roll

Pröva hela artikel 5 före godkännande. Policyexemplen är inte uttömmande och undantag kräver stöd. Fastställ om företaget är tillämpare, som förordningen kallar tillhandahållare, leverantör eller har en annan roll. Egna system, eget namn eller ändringar av ändamål och funktion kan påverka ansvaret och kräver separat bedömning. Se artiklarna 3, 5 och 25, källa 1.

Bedöm högriskklassificeringen separat

Policyns särskilda risklista är bredare än AI-förordningens högriskklassificering. Bedöm ändamål, avgränsningar och systemets övergångsregler. Rekryteringsurval, kandidatbedömning, prestationsövervakning och vissa beslut om arbetsvillkor behöver särskild prövning. All AI i undervisning eller vård är inte automatiskt högrisk. Mänsklig slutkontroll gör inte i sig ett system till lågrisk. Ta in stöd för eventuella undantag enligt artikel 6.3; profilering av personer utesluter den lättnaden.

Om högriskanvändning införs behövs ett separat upplägg inför tillämplig tidsfrist för bland annat instruktioner, mänsklig kontroll, övervakning, loggar, incidenter och föreskriven information till berörda. Pröva också om en konsekvensbedömning för grundläggande rättigheter krävs. Se artiklarna 6, 26-27, 111, 113 och bilaga III samt datumen i avsnitt 8.

Kontrollera information och märkning enligt artikel 50

- Fastställ företags roll och den aktuella funktionen. Leverantörers skyldigheter för direkt AI-interaktion och maskinläsbar märkning skiljer sig från tillämpares informationsskyldigheter. Kontrollera även köpta kundchattbotar.
- Bedöm särskilt deepfakes och AI-text som publiceras för att informera allmänheten i frågor av allmänt intresse. Syntetisk röst eller bild är inte automatiskt en deepfake. Pröva även informationskrav vid tillåten känsloligenkänning eller biometrisk kategorisering.
- Undantaget för mänsklig granskning eller redaktionell kontroll och redaktionellt ansvar gäller den nämnda textregeln. Det ger inget generellt undantag för granskade deepfakes. Pröva andra avgränsningar och undantag utifrån den konkreta användningen.
- Där information krävs ska den vara tydlig, särskiljbar, tillgänglig och lämnas senast vid första interaktionen eller exponeringen. Dokumentera ansvar, utformning och eventuellt undantag. Se artikel 50 och kommissionens vägledning, källor 1 och 5.

5 Förbered incidenthanteringen

Intern rapportering ska ske omedelbart enligt policyn. Varje AI-avvikelse är inte en personuppgiftsincident. Ansvarig funktion ska bedöma vad som hänt, begränsa skadan och vid personuppgiftsincident dokumentera händelsen, riskbedömningen, åtgärderna och när företaget fick vetskap.

- Personuppgiftsansvarig ska anmäla till behörig tillsynsmyndighet utan onödigt dröjsmål och om möjligt inom 72 timmar efter vetskap, om det inte är osannolikt att incidenten medför risk för enskildas rättigheter och friheter. Förklara en försening. Ofullständig information får kompletteras; invänta inte slutlig utredning.
- Vid sannolik hög risk ska berörda informeras utan onödigt dröjsmål, om inget tillämpligt undantag gäller.
- Är företaget personuppgiftsbiträde ska den personuppgiftsansvariga underrättas utan onödigt dröjsmål. Följ även tillämpliga avtalsfrister.

Dokumentera även incidenter som inte anmäls och skälen. Utse ansvariga för beslut, kontakter, anmälan och återstart. Se GDPR artiklarna 33-34 och IMY, källor 3 och 6.

6 Kontrollera att införandet fungerar

Policyägaren ska före start dokumentera följande som klart, inte tillämpligt med motivering eller stopp. Ange ansvarig, datum och länk till underlag för varje punkt. Åtgärda kvarstående hinder innan den berörda användningen börjar.

- Rättsliga villkor: förbud, roller, transparens, klassificering, dataskydd, avtal, arbetsmiljö och samverkan är prövade. Nödvändiga bedömningar och samråd är genomförda.
- Fungerande skydd: behörigheter, leverantörsinställningar och gallring är kontrollerade. Agenters åtgärdsgränser, godkännanden och stoppfunktion är testade.
- Rutiner och ansvar: verktygslista, kontaktvägar, rättighets- och incidentrutiner samt tillämpligt behandlingsregister är klara.
- Introduktion och övning: berörda har fått roll- och riskanpassat stöd och prövat några realistiska arbetsfall, inklusive ett felaktigt resultat och en incident. Granskare har relevant underlag, kompetens och mandat att ändra AI-förslag.
- Uppföljning: nästa kontroll och ändringar som utlöser tidigare prövning är bestämda. Följ upp faktiska problem och behov av fortsatt stöd.

Artikel 4 kräver åtgärder som stöder utvecklingen av AI-kunnighet, anpassade till sammanhanget. Dokumentera insatsernas datum, deltagare och innehåll. Ett visst kursintyg eller en viss kurslängd krävs inte, och intyg bevisar inte efterlevnad. Bestämmelsen kräver inte att en viss individuell kunskapsnivå garanteras. Företagets introduktionskrav är ett internt sätt att arbeta med detta. Se källa 1.

7 För register över godkända verktyg

Använd en post per verktyg och kontotyp. Beskriv konkret vad användaren får göra. Företaget ska kunna begränsa eller återkalla ett godkännande när villkor eller risker ändras.

Verktyg, leverantör och kontotyp: [namn och version eller plan]

Godkänd användning: [konkreta uppgifter och vilka som får utföra dem]

Tillåten information och begränsningar: [informationstyper och uttryckliga förbud]

Obligatoriska inställningar: [åtkomst, träning, lagring, radering och tillåtna kopplingar]

Roller och bedömning: [företagets AI-roll och dataskyddsroll, ändamål, prövning av förbud, transparens och risk samt länk till underlag]

Verktygsansvarig: [namn och kontaktväg]

Beslut och underlag: [beslutsfattare, datum och länk till bedömning]

Nästa kontroll: [datum och sådant som utlöser en tidigare kontroll]

Exempel på avgränsning: textutkast utifrån redan publicerad produktinformation, utan kunduppgifter och med granskning före publicering. Exemplet innebär inte att något visst verktyg är godkänt.

8 Rättsläge och källor

Kontrollerat den 10 oktober 2026. Kontrollera reglerna igen vid beslut och ändringar. EU-förordningar, svensk lag och tillämpliga AFS-föreskrifter är bindande. Myndighetsvägledning och allmänna råd är tolkningsstöd respektive rekommendationer. Konsoliderad EU-text är ett läshjälpmedel; rättsakterna i EU:s officiella tidning är autentiska.

- 2 februari 2025: AI-kunnighet och de ursprungliga förbuden började tillämpas.
- 27 juli 2026: ändringsförordning EU 2026/1744 trädde i kraft, med bland annat ändrad artikel 4. Inte alla nuvarande förbudspunkter har gällt sedan februari 2025.
- 2 augusti 2026: artikel 50 började tillämpas. Vissa äldre system har leverantörsövergång för just artikel 50.2 till 2 december 2026. Det skjuter inte upp tillämpares deepfake-information.
- 2 december 2026: nya förbud i artikel 5.1 ba-bb och relaterade bestämmelser börjar tillämpas. Pröva deras exakta räckvidd, bland annat för visst syntetiskt intimt eller sexuellt material och sexuellt övergreppsmaterial avseende barn.
- 2 december 2027 respektive 2 augusti 2028: uppskjutna högriskregler för bilaga III respektive produktanknutna system enligt artikel 6.1 börjar tillämpas. Kontrollera systemets övergångsregler särskilt. Annan tillämplig lag gäller under tiden.

GDPR-delen av Digital Omnibus, ärende 2025/0360(COD), är fortfarande ett förslag vid kontrollen och ska inte blandas ihop med den antagna AI-ändringen. Guiden använder därför GDPR:s nuvarande 72-timmarsregel.

Källor och tolkningsstöd

[Källa 1 AI-förordningen i lydelsen den 27 juli 2026](#)

[Källa 2 Ändringsförordning EU 2026/1744](#)

[Källa 3 Dataskyddsförordningen GDPR](#)

[Källa 4 IMY om GDPR vid användning av generativ AI](#)

[Källa 5 Kommissionens vägledning om transparens enligt artikel 50](#)

[Källa 6 IMY om hantering av personuppgiftsincidenter](#)

[Källa 7 Arbetsmiljöverket AFS 2023:1](#)

[Källa 8 Lag om medbestämmande i arbetslivet](#)

[Källa 9 Skadeståndslagen om arbetsgivares och arbetstagares ansvar](#)

[Källa 10 EDPB om automatiserade beslut och profilering](#)

[Källa 11 Digg om att införa en AI-policy](#)

[Källa 12 Europaparlamentets ärende 2025/0360\(COD\)](#)

Policyns ansvarsförttydligande ska läsas mot bland annat skadeståndslagen, 3 kap. 1 § och 4 kap. 1 §. Verklig mänsklig prövning stöds av GDPR artikel 22 och EDPB:s riktlinjer, men policyns generella mänskliga beslutspunkt är en strängare intern regel. Diggs material riktar sig till offentlig förvaltning; för inte över myndighetsspecifika krav automatiskt. IMY anger att dess generativ-AI-vägledning huvudsakligen också vägleder privata verksamheter.

AI-KLOK · Mallversion 1.1 · 10 oktober 2026