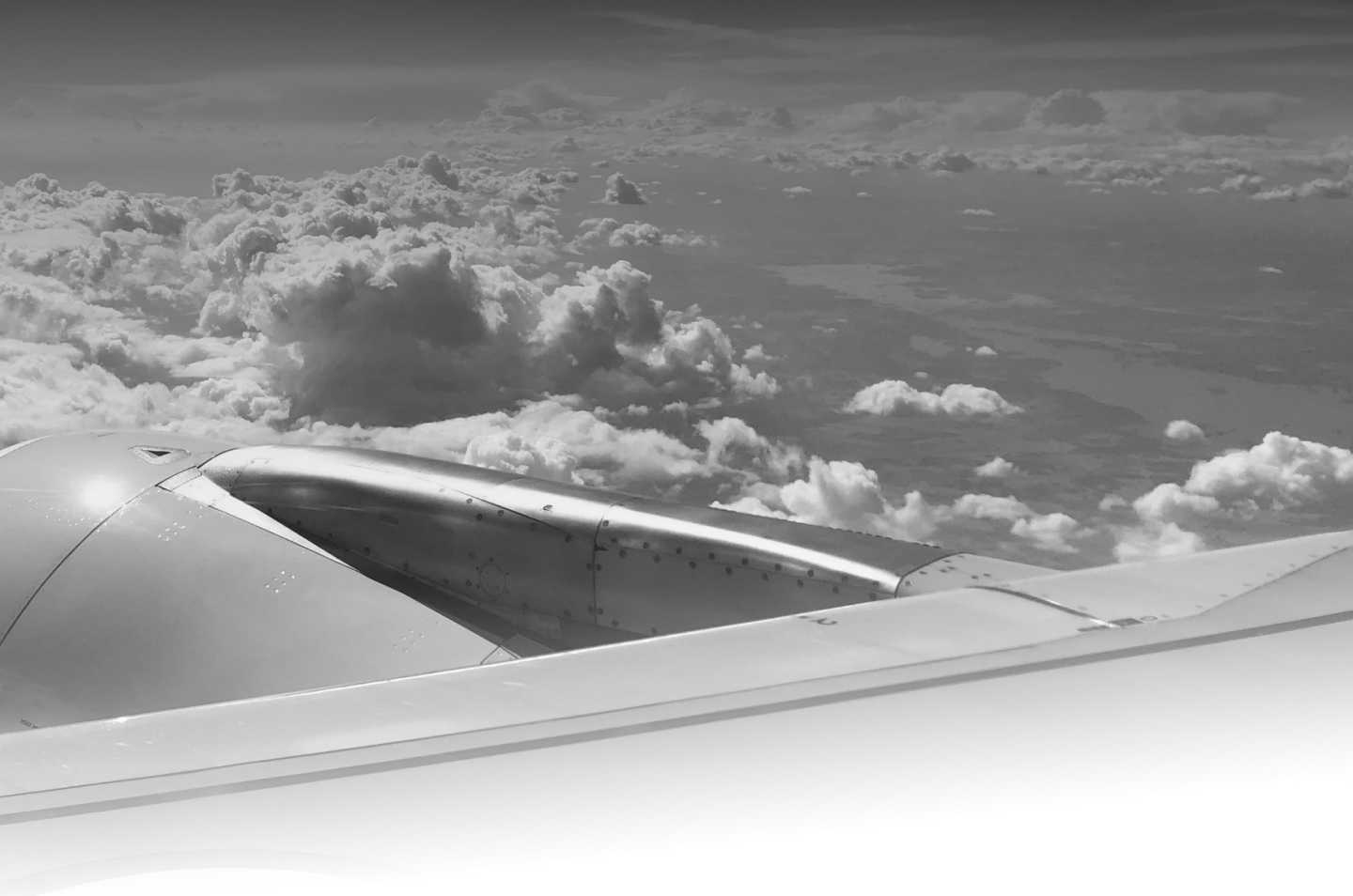


AI and policy management

Strategic AI policy for responsible use

Carin Östling & Martin Tilly
2025-04-15



TOKSTARK.

Strategisk AI policy för ansvarsfull användning



Inledning

Artificiell intelligens (AI) är idag en naturlig del av vardagen i många organisationer. Samtidigt är det vanligt att medarbetare använder egna AI-verktyg utan organisationens kännedom, vilket kan skapa stora juridiska, etiska och operativa risker. Att etablera en tydlig AI-policy är därför avgörande för att säkerställa en säker, effektiv och etisk hantering av AI.

Vad är en AI-policy?

En AI-policy är ett internt strategiskt styrdokument som beskriver riktlinjer, principer och rutiner för organisationens användning, utveckling och styrning av AI. Syftet med en AI-policy är att säkerställa att AI används ansvarsfullt och i linje med lagar, etiska riktlinjer samt organisationens övergripande strategier och mål.

Varför behövs en AI-policy?

En AI-policy hjälper organisationen att:

- Säkerställa efterlevnad av juridiska krav och regelverk.
- Skydda organisationens data, integritet och sekretess.
- Stärka varumärke och förtroende hos kunder, medarbetare och partners.
- Minimera juridiska och etiska risker som diskriminering, bristande transparens och integritetsintrång.
- Främja innovation genom att erbjuda tydliga ramar inom vilka AI kan testas och implementeras.



Framtagning av AI-policy – steg för steg

1. Kartläggning och analys av AI-användning

Genomför en detaljerad kartläggning för att identifiera vilka AI-verktyg som används inom organisationen, deras syfte, användare och datahantering. Inkludera en bedömning av nuläget och identifiera eventuella problemområden.

2. Omfattande riskbedömning

Utför en grundlig riskbedömning med fokus på juridiska aspekter (GDPR, AI Act), säkerhet (ISO 27001, NIS2-direktivet) och etik (bias, transparens). Identifiera potentiella konsekvenser och prioritera områden för insatser.

3. Utformning av riktlinjer och principer

Formulera detaljerade riktlinjer anpassade efter organisationens unika behov och riskprofil. Fastställ etiska principer samt ansvarsområden tydligt.

4. Implementering

Säkerställ att policyn kommuniceras effektivt och att medarbetare förstår och kan tillämpa riktlinjerna genom omfattande utbildningsinsatser.

5. Kontinuerlig uppföljning och revision

Utveckla systematiska processer för regelbunden granskning och revision av AI-policyn, för att hålla dokumentet aktuellt med teknologiska framsteg och regulatoriska förändringar.

Utbildning, efterlevnad och avvikelshantering

Integrerad utbildning och kommunikation

En kontinuerlig utbildningsplan bör införas där alla medarbetare utbildas regelbundet i AI-policyn. Utbildningen bör omfatta praktiska exempel, juridiska krav, etiska överväganden och organisationens specifika användning av AI.

Integration med befintliga styrdokument och kvalitetsledningssystem

AI-policyn bör integreras med relevanta existerande policydokument som IT-policy, informationssäkerhetspolicy och kvalitetsledningssystem (t.ex. ISO 9001 och ISO 27001). Detta säkerställer en enhetlig hantering av AI-frågor inom hela organisationen.

Efterlevnad och kontroll

För att säkerställa effektiv efterlevnad bör tydliga rutiner och processer införas för regelbundna interna revisioner och stickprov. Ansvarsområden för kontroll och efterlevnad ska vara klart definierade.

Avvikelsehantering

Inför en strukturerad process för hantering av avvikelser, där brister och avsteg från AI-policyn identifieras, dokumenteras, åtgärdas och följs upp. Detta inkluderar även rutiner för rapportering och transparens gentemot ledning och medarbetare.

Innehåll och framtagande



Följande stycken kan användas vid skapandet av organisationens egen AI-policy:

Introduktion och syfte

Kortfattad beskrivning av syftet med policyn och varför den behövs.

Omfattning och begränsningar

Definiera tydligt var och när policyn gäller samt eventuella begränsningar.

Ansvar och roller

Specificera tydligt vilka roller och ansvar som gäller för olika medarbetare och chefer.

Etiska principer och riktlinjer

Beskriv organisationens etiska ramverk och principer för ansvarsfull AI-användning.

Riskhantering och säkerhetsåtgärder

Ange hur risker identifieras och hanteras för att skydda data och integritet.

Integration med andra styrdokument och kvalitetsledningssystem

Förklara hur AI-policyn integreras med befintliga policydokument och kvalitetssystem.

Utbildning och kommunikationsstrategi

Definiera strategi och metoder för hur utbildning och information sprids internt.

Process för implementering och efterlevnad

Beskriv rutiner och metoder för att säkerställa att policyn implementeras effektivt.

Avvikelsehanteringsprocess

Förklara procedurer för hantering av avvikelser och icke-efterlevnad.

Rutiner för revision och uppdatering

Ange hur och när policyn ska revideras och uppdateras.



Nedan följer ett exempel på en AI-policy. Kontakta oss gärna för att få en kopia.

TOKSTARK	TOKSTARK
AI-policy för TOKSTARK AB Denna AI-policy syftar till att säkerställa att TOKSTARK AB använder artificiell intelligens på ett ansvarsfullt, etiskt, hållbart och lagligt sätt. Policyn utgår från gällande och kommande regelverk samt internationella standarder, inklusive EU:s AI Act (AI-förordningen)[1], Dataskyddsförordningen (GDPR)[2], ISO/IEC 38507[3] (styrning av AI), ISO/IEC 27001[4] (informationssäkerhet) och NIS2-direktivet[5] (cybersäkerhet och skydd av kritiska informationssystem). Policyn fungerar som ett styrande dokument för både TOKSTARKS interna AI-användning och för hur vi stödjer våra kunder i att utveckla och tillämpa AI på ett hållbart och förtroendeinbringande sätt. 1. SYFTE Policyn syftar till att: (i) skapa en gemensam förståelse för hur TOKSTARK använder AI ansvarsfullt, (ii) skydda kunderna och TOKSTARKS egna data, (iii) säkerställa efterlevnad av lagar och regler, (iv) främja innovation inom trygga ramar, (v) bidra till hållbar användning av teknik samt (vi) stärka förtroendet hos kunder, partners och medarbetare. 2. OMFATTNING Denna policy gäller alla medarbetare, konsulter, underkonsulter och underleverantörer som arbetar med och under TOKSTARKS namn – vid såväl interna aktiviteter som kunduppdrag. Kundens AI-policy gäller alltid i första hand. Om kunden inte har en AI-policy gäller TOKSTARKS policy i samråd med kunden. Policyn omfattar användningen av generativa AI-verktyg samt annan AI-teknik som används i affärsutveckling, utbildning, analys och projektledning. 3. PRINCIPER FÖR ANSVARSFULL OCH HÅLLBAR AI-ANVÄNDNING TOKSTARK tillämpar följande principer för AI-användning: • AI får endast användas som beslutsstöd – aldrig för att fatta avgörande beslut utan mänsklig inblandning. • Det ska alltid framgå när AI har använts för att ta fram underlag till kunder. • AI-genererat bildmaterial ska märkas tydligt. • AI får inte användas på ett sätt som strider mot mänskliga rättigheter eller etiska riktlinjer. • TOKSTARK förbjuder användning av AI för manipulation, diskriminering eller vilseledande syften. • TOKSTARK använder AI med hållbarhet i åtanke och strävar efter att minimera onödig resursförbrukning, till exempel genom selektiv och behovsbaserad användning av AI-genererade bilder och datagenerering. 4. DATASKYDD OCH INFORMATIONSSÄKERHET • TOKSTARK förbjuder att personuppgifter, kunddata eller sekretessbelagd information matas in i publika AI-verktyg. • TOKSTARK följer gällande GDPR-krav samt interna säkerhetsrutiner inom ramen för företagets ledningssystem. • Arbetet med informationssäkerhet och AI-styrning utgår från etablerade standarder såsom ISO/IEC 27001[4], ISO/IEC 38507[3] och de krav som ställs enligt NIS2-direktivet[5]. 5. IMPLEMENTERING OCH UTBILDNING Policyn kommuniceras till samtliga medarbetare som finns tillgänglig i kvalitetledningssystemet. En kortversion publiceras på hemsidan i syfte att vara transparent mot externa intressenter, kunder och partners. Utbildning genomförs årligen i samband med revision av policyn för att säkerställa aktualitet, förståelse och efterlevnad. 6. POLICYANSVAR OCH EFTERLEVNAD TOKSTARKS VD är ansvarig för att policyn efterlevs och uppdateras vilket görs på årsbasis. Incidenter som rör otillbörlig AI-användning ska rapporteras enligt TOKSTARKS process för incidenthantering. Policyn revideras och aktualiseras på årsbasis eller vid behov utifrån ny teknik, lagstiftning eller kundkrav. Vid	uppdatering tas hänsyn till förändringar i AI-förordningen, dataskyddslagstiftning, internationella standarder och nationella cybersäkerhetsdirektiv och ny lagstiftning. 7. DEFINITIONER AI-SYSTEM (enligt AI Act, 2024/1689): Ett maskinbaserat system som är utformat för att fungera med varierande grad av autonomi och som, för angivna mål, kan generera utdata såsom förutsägelser, rekommendationer eller beslut baserat på indata den tar emot. 8. RELATION TILL ANDRA POLICYS OCH STYRANDE DOKUMENT Denna AI-policy är en del av TOKSTARKS integrerade ledningssystem och ska tillämpas tillsammans med följande styrande dokument: Kvalitetssystem (QMS) – Policyn stödjer kvalitetssystemets struktur för uppföljning och förbättringsarbete. • Kvalitetspolicy – Principerna om struktur, leverans och ansvar återspeglas i denna policy, särskilt vad gäller laguppfyllelse och rätt kvalitet i tid. • Personal Data Management Policy – Policyn harmoniseras med hantering av personuppgifter enligt GDPR och kompletterar regler för dataminimering, incidentrapportering och datasäkerhet. • Code of Conduct – AI-policyn vilar på samma etiska grund som TOKSTARKS uppförandekod och följer dess riktlinjer kring mänskliga rättigheter, transparens och ärlighet i affärsrelationer. 10. RIKTLINJER Riktlinjer för AI-användning inom TOKSTARK Innan AI används i ett projekt eller arbetsmoment ska följande riktlinjer följas: - Följer AI-användningen och verktyget TOKSTARKS policy, kundens policy och gällande lagstiftning? - Delas känsliga uppgifter, personuppgifter eller kunddata? (Om ja – avbryt.) - Är innehållet kontrollerat och försett av en människa innan det används? - Är AI-användningen tydligt markerad i dokument, bild eller beslutsunderlag? - Är användningen etiskt motiverad, främjar icke-diskriminering, undviker bias och lagras inom EU? 11. Q&A A. Använder TOKSTARK AI i sina leveranser? Ja, vi använder AI som ett stöd i analys, planering och dokumentation. All AI-användning granskas av en konsult innan leverans. B. Delar ni kunddata i AI-system? Nej, TOKSTARK har tydliga rutiner som förbjuder att kunddata, personuppgifter eller känslig information delas i publika AI-verktyg. Detta följer riktlinjerna i GDPR[2] och våra interna säkerhetsrutiner. C. Hur säkerställer ni att AI-användningen följer lagar och regler? Vi följer EU:s AI Act[1] och GDPR[2]. Vi har interna utbildningar och ett ledningssystem som stödjer detta, samt utgår från standarder som ISO/IEC 27001[4] och ISO/IEC 38507[3]. D. Hur hanterar ni risker som bias och felaktigheter? AI används aldrig för att fatta kritiska beslut. Alla resultat granskas och kontrolleras innan användning för att säkerställa transparens och rättvisa enligt våra etiska riktlinjer. E. Vem ansvarar för att AI används korrekt hos er? Vår VD är policyansvarig, men alla medarbetare har ansvar att följa riktlinjerna och rapportera avvikelser. F. Kan vi som kund få tillgång till er policy? Ja. Vår policy finns i konverterad på hemsidan och full version på begäran. 12. REFERENSER [1] Europaparlamentet och Rådet: AI Act (EU 2024/1689) [2] Europaparlamentet och Rådet: Dataskyddsförordningen (GDPR) [3] ISO/IEC 38507:2019 Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organizations [4] ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection [5] Europaparlamentet och Rådet: NIS2-direktiv (EU) 2022/2555



”En AI-policy är ett levande verktyg och dokument för att styra och stödja ansvarsfull AI-användning”

Avslutning

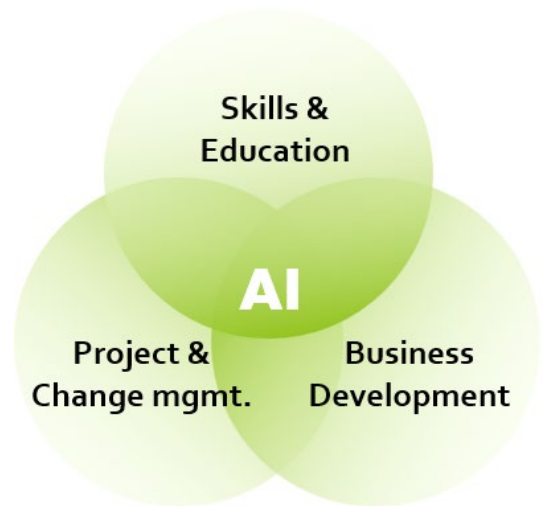
En AI-policy är ett levande verktyg och dokument för att styra och stödja ansvarsfull AI-användning. Genom aktiv ledningsförankring och tydlig integrering med övriga styrsystem blir policyn ett viktigt stöd i verksamhetens arbete med AI. Att kontinuerligt granska, följa upp och förbättra policyn säkerställer långsiktig framgång och hållbarhet.

About TOKSTARK●

When you want to increase your efficiency, TOKSTARK supports you with AI advantage.

We provide services with the goal of making you more efficient with AI..

Our goal is to be proud of what we achieve together while enjoying the process. We exist because we are a trustworthy partner committed to our partners success while being easy to collaborate with.



Team TOKSTARK.



Daniel Karlsson PhD
Sr AI Advisor

Experienced project leader with passion to empowering individuals and organizations to achieve their objectives through the pillars of transparency, efficiency, and trust. With a robust background in the life sciences-, technical-, and IT sectors, Daniels career spans various roles within companies of different sizes and stages of their development journey.



Carin Östling MPH
Sr AI Transformation Strategist

As a leader in change, I strive to make every step toward the goal both inspiring and meaningful. I am humble and driven, with a strong passion for leading through change processes and developing both organizations and people. My focus is on creating the best conditions for success and ensuring that deliveries maintain high quality and long-term sustainability.



Martin Tilly MSc & BBA
Sr Project Leader

Described as a hardworking and result-driven person, with a strong track record of managing several strategic corporate projects at international companies. Martin loves to deliver result through inspiring others to join up towards a common goal.

TOKSTARK●COM