SÅ HÄR GÖR VI I NACKA
AI

Diarienummer	Fastställd/senast uppdaterad	Beslutsinstans	Ansvarigt politiskt organ	Ansvarig processägare
KFKS-2026-00434	2026-04-24	Stadsdirektör	Kommunstyrelsen	Digitaliseringsdirektör
Så här gör vi i Nacka	AI			

AI

Dokumentets syfte

Handledningens syfte är att ge en praktisk vägledning till hur AI kan utforskas och användas i kommunens verksamhet på ett systematiskt, riskavvägt, robust och ansvarsfullt sätt, i linje med Nacka kommuns policy för AI-användning och därtill kopplade styrdokument.

Dokumentet gäller för

Samtliga medarbetare och förtroendevalda i kommunen och de kommunala bolagen.

Inledning

AI (artificiell intelligens) bygger på att datorsystem tränar på stora mängder data och lär sig utföra olika sorters uppgifter som underlättar vardagen för oss människor.

I Nacka kommun är vi utforskande och nyfikna på att utveckla arbetssätt med hjälp av ny teknik, och ser stora möjligheter med AI. Samtidigt måste vi vara ansvarsfulla när vi utforskar de nya möjligheter som tekniken ger. Vi måste alltid vara medvetna om riskerna som ny teknik medför, men också ha insikt i de möjligheter som dessa erbjuder oss.

Detta dokument är till för att hjälpa dig som medarbetare att förstå hur du kan använda AI i arbetet på ett ansvarsfullt sätt.

Att använda AI-tjänster

Det finns en stor potential i användningen av AI. Därför är det också viktigt att AI nyttjas på ett ansvarsfullt sätt för att säkerställa att dess tillämpningar inte orsakar felaktigheter, skada eller orättvisa.

Ansvaret gäller oavsett om du använder allmänt tillgängliga AI-tjänster eller AI-funktioner i system som kommunen köpt in, som beskrivet under rubriken ”Anpassade AI-tjänster” i detta dokument.

Oavsett i vilket syfte eller i vilket sammanhang du använder en AI-tjänst i arbetet behöver du alltid komma ihåg att

- du ansvarar för den information du matar in i en AI-tjänst
- du ansvarar för hur resultatet av AI-tjänsten används
- du behöver granska och eventuellt rätta felaktigheter i den information som produceras av AI-tjänsten du använder
- du ska rapportera eventuella avvikelser, fel eller missbruk enligt kommunens kanaler för incidentrapportering för informationssäkerhet och dataskydd
- du som lyder under lagstadgad tystnadsplikt behöver särskilt noggrant avgränsa i vilka sammanhang du kan använda AI-tjänster i arbetet

Dessa förhållningssätt gäller både för användning av allmänt tillgängliga AI-tjänster och för anpassade AI-tjänster.

Allmänt tillgängliga AI-tjänster

Vid användningen av verktyg som är allmänt tillgängliga är det viktigt att komma ihåg att den data som matas in till verktyget oftast lagras av de olika tjänsteleverantörerna. Om känslig information delas innebär det därför en risk för oavsiktlig delning mot tredje part, vilket leder till förlust av konfidentialitet och risk för lagbrott. Därför är det endast tillåtet att dela öppen information i allmänt tillgängliga AI-tjänster.

Allmänt tillgängliga AI-tjänster får bara användas med öppen information, t. ex. sådant som redan finns publicerat på öppet åtkomliga hemsidor.

Anpassade AI-tjänster

Till skillnad från allmänt tillgängliga AI-tjänster kan andra förutsättningar råda när AI används i en process som stöds av ett system som kommunen upphandlat, det vi här benämner som ”anpassade AI-tjänster”.

Möjligheter kan alltså finnas att använda anpassade AI-tjänster även för bearbetning av information som inte får användas i allmänt tillgängliga AI-tjänster, om säkerhetstekniska förutsättningar finns.
För att avgöra om detta kan ske ska AI-tjänsten utvärderas enligt processen för beredning av digitaliseringsärenden.

Uppgifter som omfattas av sekretess eller annan känslig information kan behandlas inom ramen för av kommunen upphandlad anpassad AI-tjänst, om det säkerställts att tjänsten uppfyller relevanta regelverk, kommunens säkerhetstekniska krav och att kommunen har laglig grund för behandlingen när AI används.

För att anpassade AI-tjänster ska kunna tas i bruk ska de klassificeras och hanteras genom processen för beredning av digitaliseringsärenden enligt kapitlet ”Att anskaffa, skapa och införa AI-tjänster”.

Informationssäkerhet och dataskydd

För AI-tjänster, precis som för andra digitala lösningar som tas i bruk i kommunen, ska kommunen tillämpa ett systematiskt och riskavvägt arbetssätt. Det innebär att behandling av Nacka kommuns information i en AI-tjänst, om den inte faller inom ramen för så kallad öppen information, ska föregås av systematiskt informationssäkerhetsarbete. Informationsklassning, risk- och konsekvensanalys samt säkerhetsåtgärder som syftar till att minska riskerna med användningen av tjänsten ska genomföras. En grundförutsättning för att du som medarbetare ska kunna tillämpa ett riskavvägt arbetssätt är att du har gått de kurser som kommunen ställt krav på för att öka säkerhetsmedvetandet.

Varje verksamhet ansvarar för att all informationsbehandling görs i enlighet med informationssäkerhetsstrategin och att medarbetarna har gått avsedda kurser.
Kontakta säkerhetsenheten vid behov av stöd.

Informationssäkerhet vid anpassade AI-tjänster

När kommunen anskaffar eller utvecklar system ska vi ställa krav på systemet utifrån vilka säkerhetsåtgärder som krävs för att information ska kunna hanteras i det. Vid anskaffning av AI-tjänster krävs särskilt övervägande hur lämpliga krav kan ställas på hur AI-modellen är utvecklad, hur ansvaret ska regleras och vilka granskningskriterier som är relevanta för att värdera leverantörens AI-teknik.

Kommunen behöver också vara medveten om hur AI-tjänsten och dess leverantör kan komma åt och behandla den information som användare matar in, så att inte kommunens information oavsiktligt riskerar att spridas vidare öppet till andra användare.

Vid anskaffning av anpassade AI-tjänster ska särskild riskutvärdering göras.

Personuppgiftsbehandling

Dataskyddsförordningen (GDPR) ska tillämpas när AI-användning innebär behandling av personuppgifter. Varje behandling av personuppgifter måste ha en rättslig grund enligt dataskyddsförordningen. För offentlig verksamhet är den rättsliga grunden i de flesta fall att kommunen utför en uppgift av allmänt intresse. Generativ AI är då ett verktyg för att utföra verksamhetens uppdrag, inte ett ändamål i sig. Om användningen av AI bidrar till att effektivisera eller stödja verksamhetens uppgifter kan det därför finnas stöd för att behandla personuppgifter med sådan teknik.

Ju större risker behandlingen innebär för den enskildes integritet, desto högre krav ställs dock på det rättsliga stödet och på de skyddsåtgärder som vidtas. Vid osäkerhet ska enhetens dataskyddssamordnare kontaktas innan användning.

Personuppgifter i allmänt tillgängliga AI-tjänster

Tänk på att det finns mer information än namn som kan göra att det går att identifiera en person: telefonnummer, arbetsplats, utbildning, och så vidare. Vissa uppgifter som t ex röst och ansikte kopplat till en person (biometriska uppgifter) kan vara särskilt känsliga att använda. Det är därför viktigt att vara försiktig och minimera den eventuella information som delas för att skydda integriteten och säkerheten för både dig och andra, eftersom kommunen inte har samma kontroll över hur uppgifterna behandlas i allmänt tillgängliga AI-tjänster.

När du använder en allmänt tillgänglig AI-tjänst ska du i största utsträckning undvika att dela personuppgifter i verktyget. Eftersträva att minimera dem till att enbart omfatta det du behöver ange för att kunna hantera ett användarkonto. Dela över huvud taget inte andras personuppgifter.

Dela inte uppgifter som är känsliga eller omfattas av sekretess

Känsliga personuppgifter eller uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (OSL) får inte delas i allmänt tillgängliga AI-tjänster. Har du behov av att kunna arbeta med denna typ av information i en AI-tjänst behöver AI-tjänsten först utvärderas enligt kapitlet ”Att anskaffa, skapa och införa AI-tjänster”.

Med AI öppnas dessutom nya möjligheter för att till exempel hitta mönster och tolka större mängder data. Det är därför viktigt att särskilt tänka på att du enligt OSL inte får samköra data mellan förvaltningar i olika nämnder hur som helst. Enskilda uppgifter, som var för sig inte omfattas av sekretess, kan i sammanslagen form utgöra sekretessbelagd information.

Om det finns behov av att kunna arbeta med känsliga uppgifter eller sekretess behöver AI-tjänsten först utvärderas enligt kapitlet ”Att anskaffa, skapa och införa AI-tjänster”.

Tänk också på att information som var för sig inte omfattas av sekretess kan komma att göra det i sammanslagen form.

Förtroende och transparens

Material som är genererat eller bearbetat med AI ska ses som ett utkast och ska alltid granskas innan det används. Du som avsändare ansvarar för innehållet och hur resultatet används, som om du hade producerat det helt själv.
Som huvudregel ska vi vara transparenta med AI-användning när material delas externt eller används i sammanhang som kan påverka medborgare.

När AI används i direkt interaktion med människor ska det framgå att användaren interagerar med AI-genererat innehåll.

Om kommunen publicerar eller sprider AI-genererat eller AI-manipulerat bild-, ljud- eller videoinnehåll som på ett märkbart sätt liknar verkliga personer, platser eller händelser ska det märkas tydligt så att mottagaren förstår att innehållet är artificiellt eller manipulerat. Märkning ska ske på ett sätt som är lätt att uppfatta (t.ex. bildtext eller tydlig notis i anslutning till innehållet). Ansvarig avsändare ska säkerställa att sammanhang och presentation inte riskerar att vilseleda.

När AI används i interaktion med människor ska vi säkerställa transparens, så att användaren förstår att den interagerar med AI-genererat innehåll.

Myndighetsutövning med hjälp av AI

För att säkerställa transparens och spårbarhet är det viktigt att kunna förstå och förklara hur beslut fattas, och om AI-tjänster är inblandade i processen. Om AI används i någon del av arbetet fram till ett beslut ska det vara tydligt vilken roll AI har haft och vilka delar som har bedömts av en människa. Verktyget som används ska, i den utsträckning det krävs för verksamheten, möjliggöra begripliga förklaringar till varför ett visst resultat har föreslagits. Den enskilde ska kunna få information om hur ärendet som helhet hanteras och vart frågor eller klagomål kan vändas.

Kom ihåg att det ska finnas begripliga förklaringar till på vilka grunder beslut fattas. Vid behov ska du som användare kunna ge förståelig och meningsfull information om underlagen till beslut.

Likabehandling, etik och moral

Likabehandlingsprinciper är avgörande för att säkerställa att AI-system inte leder till diskriminerande eller orättvisa resultat. Olika modeller är tränade på olika data och kommer, liksom människor, vara partiska på olika sätt. Det är viktigt att vara medveten om detta, då du som medarbetare ansvarar för resultatet av det AI producerar. Du behöver granska det AI producerat utifrån risken att det kan vara grundat på snedvridna principer som gör det diskriminerande eller oetiskt

Om du använder AI i undervisningssammanhang ska du särskilt tänka på att inkludera etiska aspekter med AI-användning för att utveckla elevernas källkritiska kompetens, exempelvis vilka källor olika AI-baserade resultat bygger på, rimlighet, eventuella felaktigheter, begränsningar och fördomar.

När, och på vilket sätt, AI används i en verksamhet måste alltså etiska och moraliska aspekter vägas in. Verksamheten behöver identifiera om det finns risker för snedvridning, och hur dessa kan upptäckas. Resultat ska följas upp och användningen ska kunna pausas om oönskade effekter uppstår.

Avvägning av hur AI kan tillämpas ur etiska och moraliska aspekter avgörs bäst av verksamheten själv. Skulle osäkerhet eller meningsskiljaktigheter ur dessa aspekter uppstå, ska befintliga processer för eskalering användas.

Att anskaffa, skapa och införa AI-tjänster

Användning av allmänt tillgängliga AI-tjänster begränsas starkt av framför allt vilken information du har möjlighet att dela legalt. De är heller inte en del av kommunens infrastruktur och kan därför bara användas som separata fristående verktyg. För att möta de behov som inte täcks in av allmänna AI-tjänster behöver AI-tjänsten upphandlas och eventuellt anpassas efter särskilda krav.

Roller enligt AI-förordningen

När vi anskaffar och använder AI måste vi förstå vår roll enligt AI-förordningen, eftersom det avgör vilket ansvar och vilka krav som gäller. Två viktiga begrepp i AI-förordningen är leverantör och tillhandahållare (se appendix).

Eftersom leverantören ansvarar för att AI-tjänsten uppfyller alla krav i AI-förordningen, medför denna roll de mest omfattande skyldigheterna. Tillhandahållare har fortfarande ansvar för att AI-tjänsten används korrekt, men regelverket är mindre omfattande än för leverantörer.

Det är därför viktigt att tidigt avgöra vilken roll vi antar i anskaffandet och användandet av en AI-tjänst.

Klassificering av AI-tjänster

När kommunen ska besluta om att anskaffa, skapa eller införa en AI-tjänst tar vi hänsyn till EU:s AI-förordning och klassificering av AI-tjänster i fyra riskkategorier:

- **Oacceptabel risk**: AI-tjänst som utgör ett tydlig hot mot säkerhet, försörjning och grundläggande rättigheter. Tjänster i denna kategori är olagliga enligt AI-förordningen och får inte användas.
- **Hög risk**: AI-tjänst som påverkar viktiga delar av samhället (t.ex. kritisk infrastruktur, utbildning, rättsväsende) kräver striktare reglering och övervakning.
- **Begränsad risk**: Dessa system kräver särskilda transparenskrav, som exempelvis att informera användare om att de interagerar med AI.
- **Minimal risk**: AI-tjänst som utgör en liten eller ingen risk omfattas inte av specifika krav, men informationssäkerhetsåtgärder och god dokumentation för framtidssäkring förordas.

Observera att det är leverantören av en AI-tjänst som ansvarar för att klassificera AI-tjänsten, men vi som kommun kan göra en annan bedömning beroende på tilltänkta användningsområden.

För oss i Nacka kommun innebär detta att vi intar följande förhållningssätt för anskaffade AI-tjänster:

- Inför att kommunen anskaffar en AI-tjänst hanteras det genom Nacka kommuns process för beredning av digitaliseringsärenden och därigenom rekommenderade åtgärder.
- De åtgärder som ska vidtas skiljer sig åt beroende på AI-tjänstens klassificering och vilken roll vi antar enligt AI-förordningen. Informationsägaren är ansvarig för att åtgärder genomförs.
- Tjänster som kategoriseras som ”Hög risk” omfattas av särskilda krav enligt AI-förordningen. De får endast tas i bruk efter att hänsyn tagits till rekommendationer lämnade av beredningsgruppen.
- I Bilaga A-C finns checklistor för begränsad respektive hög risk när kommunen antar rollen som tillhandahållare.

För behov som inte täcks av allmänt tillgängliga AI-tjänster behöver specifik AI-tjänst upphandlas, och eventuellt anpassas efter särskilda krav.

Har du eller din verksamhet ett sådant behov ska det skickas in till kommunens process för beredning av digitaliseringsärenden.

Interoperabilitet och flexibilitet

När kommunen avser upphandla och införa en anpassad AI-tjänst är det viktigt att eftersträva interoperabilitet, alltså att tjänsten fungerar smidigt ihop med de system kommunen redan använder och enkelt kan kommunicera med andra verktyg. Tjänsten bör också vara flexibel, så att den går att anpassa om behov förändras eller när det kommer nya tekniska möjligheter.

Du som projektägare ansvarar för att säkerställa att denna typ av förmågor inkluderas i upphandlingen av en anpassad AI-tjänst. Ta gärna stöd av digitaliseringsenheten för formulering av tekniska krav.

Appendix: Definitioner

Artificiell intelligens (AI): AI är ett datorprogram som tar emot information, analyserar den och sedan gör något med den, som att förutse vad som kan hända, skapa innehåll, ge förslag eller fatta beslut. Det kan påverka både verkliga och digitala miljöer, beroende på vad det används till.

AI-tjänster: Med ordet "tjänster" avses appar, programvaror samt andra digitala tjänster och verktyg. Med "AI-tjänster" avses tjänster som innehåller större eller mindre inslag av artificiell intelligens.

Generativ (skapande) AI: AI-tjänster som skapar nytt material baserat på enkla instruktioner kallas för generativ AI. Det finns en stor mängd AI-baserade datorprogram, system och IT-tjänster som genererar nytt material i form av till exempel text, bild, video och programmeringskod. Det finns ingen direkt definition av "generativ AI" i AI-förordningen, men man kan utgå ifrån definitionen för AI för allmänna ändamål som överensstämmer till stor del.

Allmänt tillgängliga AI-tjänster: AI-tjänster som är tillgängliga för vem som helst att använda t.ex. via webbsida eller via en app, som t ex ChatGPT, Sana AI eller Midjourney. Allmänt tillgängliga AI-tjänster är **inte** anskaffade, skapade eller införda specifikt för kommunens behov och är därför inte heller granskade av kommunen.

Anpassade AI-tjänster: AI som är anskaffad, skapad eller införd specifikt för kommunens behov och i enlighet med kommunens krav.

GPAI eller **AI-modeller för allmänna ändamål**: En GPAI är en kraftfull språkmodell som tränats på stora mängder data för att kunna utföra många typer av uppgifter.

Leverantör enligt AI-förordningen är den som utvecklar, tillhandahåller eller ändrar ett AI-system på ett sätt som påverkar dess funktion eller syfte. Man räknas som leverantör om man:

- Utvecklar en AI-tjänst eller en AI-modell för allmänna ändamål.
- Släpper ut AI-tjänsten på marknaden eller börjar använda det i eget namn eller under eget varumärke.
- Gör en väsentlig ändring av en AI-tjänst, exempelvis genom att förändra dess funktion på ett sätt som påverkar hur det följer AI-förordningen.
- Ändrar det avsedda ändamålet så att en AI-tjänst som tidigare inte var högrisk nu klassificeras som ett högrisksystem.

Tillhandahållare enligt AI-förordningen är en organisation som använder en AI-tjänst inom sin verksamhet, men utan att förändra den på ett sätt som gör att den räknas som en ny produkt.

Öppen information: Information som är tillgänglig för alla utan några begränsningar. En användbar liknelse kan vara: ”information som kan läggas öppet tillgänglig på en webbsida eller i sociala medier”.

Känsliga personuppgifter: Uppgifter om ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i en fackförening, hälsa, en persons sexualliv eller sexuella läggning, genetiska uppgifter och biometriska uppgifter som entydigt identifierar en person.

Integritetskänsliga personuppgifter: Uppgifter som på grund av sin karaktär är extra viktiga att skydda, även om de inte definieras som känsliga personuppgifter i Dataskyddsförordningen. Hit räknas dels identifierande personuppgifter såsom namn och personnummer. Dels vissa uppgifter om ekonomiska förhållanden, omdömen och värderingar av en person såsom social förmåga, inlärningsförmåga och liknande, provresultat, resultat av personlighetstester och annan information som ligger nära den privata sfären är exempel på integritetskänsliga personuppgifter.

Bilaga A – Checklista för tillhandahållare, begränsad risk

När vi anskaffar och använder en AI-tjänst som klassas som begränsad risk har vi som tillhandahållare ansvar för att säkerställa ansvarsfull användning, med särskilda krav om transparens enligt AI-förordningen.

Utöver de bindande kraven uppmuntras organisationer att följa god praxis, till exempel genom att dokumentera syfte och begränsningar, vilket bidrar till ansvarsfull användning. Därför rekommenderas nedan aktiviteter som minimum vid begränsad risk.

Texten i detta dokument är endast en kort förklaring, för fullständig beskrivning av kraven hänvisas till respektive artikel i AI-förordningen. Se referens inom parentes.

☐ **Säkerställ att informationsklassning är gjord**
Den information som avses hanteras i AI-tjänsten ska vara informationsklassad, så att eventuella säkerhetsåtgärder kan vidtas vid behov för korrekt hantering. Observera att riskklassificeringen av AI-tjänsten som helhet kan förändras beroende på vilken typ av information och eventuella personuppgifter som avses hanteras i den.

☐ **Se till att användning sker i enlighet med kommunens styrdokument**
Användning av generativ AI ska alltid ske enligt ”Så här gör vi i Nacka – AI”, inklusive krav på informationssäkerhet, etiska riktlinjer och kontroll av resultat.

☐ **Transparens och märkning vid användning** (Art. 50)
Informera slutanvändare när de interagerar med AI eller när innehåll har genererats/manipulerats av AI (till exempel text, bild, ljud eller video).
Det ska tydligt framgå med märkning att innehållet är AI-genererat, om det på ett märkbart sätt liknar verkliga personer, platser eller händelser.

Bilaga B – Checklista för tillhandahållare, GPAI med begränsad risk

Även om AI-förordningen huvudsakligen riktar sig till leverantörer av GPAI-modeller, har också tillhandahållare ett ansvar när de använder dessa modeller. Tillhandahållaren ska säkerställa korrekt användning enligt leverantörens instruktioner för att minimera risker och säkerställa ansvarsfull användning. Observera att ytterligare åtgärder och ansvar tillkommer om användningen bedöms som hög risk.

Texten i detta dokument är endast en kort förklaring, för fullständig beskrivning av kraven hänvisas till respektive artikel i AI-förordningen. Se referens inom parentes.

☐ **Säkerställ att informationsklassning är gjord**
Den information som avses hanteras i AI-tjänsten ska vara informationsklassad, så att eventuella säkerhetsåtgärder kan vidtas vid behov för korrekt hantering. Observera att riskklassificeringen av AI-tjänsten som helhet kan förändras beroende på vilken typ av information och eventuella personuppgifter som avses hanteras i den.

☐ **Se till att användning sker i enlighet med kommunens styrdokument**
Användning av generativ AI ska alltid ske enligt ”Så här gör vi i Nacka – AI”, inklusive krav på informationssäkerhet, etiska riktlinjer och kontroll av resultat.

☐ **Transparens och märkning vid användning** (Art. 50)
Informera slutanvändare när de interagerar med AI eller när innehåll har genererats/manipulerats av AI (till exempel text, bild, ljud eller video).
Det ska tydligt framgå med märkning att innehållet är AI-genererat, om det på ett märkbart sätt liknar verkliga personer, platser eller händelser.

☐ **Använd enligt instruktioner** (Art. 53.1b)
Säkerställ att AI-tjänsten (inkluderat GPAI-modeller) används i enlighet med den tekniska dokumentation och begränsningar som leverantören har tillhandahållit.

☐ **Dokumentation från leverantören** (Art. 53-55)
Begär och säkerställ att leverantören kan visa bevis på hur de uppfyller sina skyldigheter enligt artiklarna 53–55, exempelvis teknisk dokumentation och riskbedömningar.

☐ **Användning i högrisk-klassificering** (Art. 26)
Om AI-tjänsten (inkluderat GPAI-modeller) avses användas eller integreras i högrisk-klassificerade områden, ska vi som tillhandahållare uppfylla alla skyldigheter för högrisk-system inklusive loggning, mänsklig översyn och incidentrapportering. Se checklista för tillhandahållare system med hög risk.

Bilaga C – Checklista för tillhandahållare, hög risk

Om en AI-tjänst klassificeras som hög risk omfattas tillhandahållaren av särskilda skyldigheter enligt artikel 26 i AI-förordningen.

Tillhandahållaren ansvarar för att använda systemet i enlighet med leverantörens instruktioner, övervaka dess drift och säkerställa att användningen inte äventyrar hälsa, säkerhet eller grundläggande rättigheter. Dessutom krävs rutiner för dataskydd, informationssäkerhet, loggning, incidentrapportering samt samarbete med myndigheter.

Denna checklista ger en sammanfattning av de skyldigheter som gäller för tillhandahållare vid hög risk.

Texten i detta dokument är endast en kort förklaring, för fullständig beskrivning av kraven hänvisas till respektive artikel i AI-förordningen. Se referens inom parentes.

☐ **Säkerställ att alla data som används är informationsklassad**
Den information som avses hanteras i AI-tjänsten ska vara informationsklassad, så att eventuella säkerhetsåtgärder kan vidtas vid behov för korrekt hantering. Det är av särskild vikt att data som matas in ska vara relevanta, tillförlitliga och motsvara systemets avsedda användningsområde.

☐ **Använd enligt instruktioner** (Art. 53.1b)
Säkerställ att AI-tjänsten används i enlighet med den tekniska dokumentation och de begränsningar som leverantören har tillhandahållit.

☐ **Behörig personal och mänsklig översyn** (Art. 26.2)
Tillhandahållaren ska se till att systemet endast används av personal med rätt kompetens och utbildning, samt utse personer som ansvarar för övervakning och kan ingripa vid behov.

☐ **Drift och övervakning** (Art. 26.2)
Säkerställ löpande övervakning av funktioner och resultat för att upptäcka eventuella avvikelser och risker.

☐ **Incidentrapportering** (Art. 26.5)
Se till att det finns en rutin för eventuella incidenter relaterat till användningen av AI-tjänsten. Om risker eller klagomål uppstår ska användningen kunna pausas och utredas.

☐ **Loggning och spårbarhet** (Art. 26.6)
Tillhandahållaren ska i minst sex månader bevara och vid behov granska loggar som genereras av systemet för att möjliggöra spårbarhet.

☐ **Transparens vid användning** (Art. 50 och art. 26.7 och 26.11)
Informera användare att de interagerar med AI eller när innehåll har genererats/manipulerats av AI (till exempel text, bild, ljud eller video). Slutanvändare och berörda arbetstagare ska informeras på ett klart och tydligt sätt när de interagerar med en AI-tjänst med hög risk.

☐ **Kontroll av registrering EU-databas** (Art. 26.8)
Kontrollera att AI-systemet med hög risk finns registrerat i EU:s databas innan användning; om registrering saknas får systemet inte användas.

☐ **Dataskydd och integritet** (Art. 27)
Om personuppgifter behandlas ska tillhandahållare genomföra en särskild konsekvensbedömning av AI-tjänstens inverkan på grundläggande rättigheter i enlighet med artikel 27. Underlag och beslut ska arkiveras så att kommunen i efterhand kan visa hur risker har hanterats

☐ **Dokumentation från leverantören** (Art. 53-55)
Begär och säkerställ att leverantören kan visa bevis på hur de uppfyller sina skyldigheter enligt artiklarna 53–55, exempelvis teknisk dokumentation, sammanfattning av träningsdata och riskbedömningar.

☐ **Se till att användning sker i enlighet med kommunens styrdokument**
Användning av generativ AI ska alltid ske enligt ”Så här gör vi i Nacka – AI”, inklusive krav på informationssäkerhet, etiska riktlinjer och kontroll av resultat.