

Uppdrag att främja offentlig förvaltnings förmåga att använda artificiell intelligens

I2021/01825

Förord

I juni 2021 fick Arbetsförmedlingen, Bolagsverket, Myndigheten för digital förvaltning (Digg) och Skatteverket i uppdrag att gemensamt genomföra ett arbete för att främja offentlig förvaltnings förmåga att främja artificiell intelligens (AI) i syfte att stärka Sveriges välfärd och konkurrenskraft. Digg fick i uppdrag att samordna arbetet.

Till uppdraget har en myndighetsgemensam styrgrupp varit knuten. Styrgruppen har bestått av följande personer:

- Patrick Eckemo och David Magård från Bolagsverket.
- Från Digg har Mats Snäll deltagit fram till i maj 2022 då Viktoria Hagelstedt och Evelina Mikaelsson tog över. I augusti 2022 avslutade Viktoria Hagelstedt sitt arbete i styrgruppen.
- Skatteverket har företrätts av Göran Sundin, fram till i augusti 2022 då Rebecca Filis tog över.
- Arbetsförmedlingen har Beatrice Sablone deltagit fram till i november 2022, då hon ersattes av Karolina Jedzejewska.

Beslut om denna rapport har fattats av generaldirektörerna för Arbetsförmedlingen, Bolagsverket, DIGG och Skatteverket.

Theodor Andersson, Digg, David Magård, Bolagsverket, Dan Nordell, Skatteverket och Andreas Henningsson, Arbetsförmedlingen har varit föredragande.

Anna Eriksson

Anna Eriksson
Generaldirektör, Digg

Maria Mindhammar
Generaldirektör, Arbetsförmedlingen

Annika Stenberg
Generaldirektör, Bolagsverket

Katrin Westling Palm
Generaldirektör, Skatteverket

Stockholm den 20 januari 2023

Sammanfattning

Artificiell intelligens (AI) är ett område med stor potential att förbättra samhället. Tidigare utredningar har visat att den beräknade nyttan av AI inom offentlig förvaltning uppgår till 140 miljarder årligen. Nyttan beräknas i form av högre produktivitet, ökade intäkter och minskade utbetalningar. AI används redan i dag i allt större utsträckning och nya AI-baserade tjänster har nyligen blivit världsnyheter utifrån deras förmågor att stötta människor i att skapa konst, utveckla kod eller ta fram utbildningsmaterial oerhört snabbt.

Regeringen anser att det är viktigt att lösningar och verktyg som utvecklas inom offentlig förvaltning kommer till nytta inom hela den offentliga förvaltningen. Mot denna bakgrund beslutade regeringen i juni 2021 att ge Arbetsförmedlingen, Bolagsverket, Digg och Skatteverket (myndigheterna) i uppdrag att främja offentlig förvaltnings användning av AI.

Denna rapport är återrapporteringen av uppdraget.

Deltagande myndigheter i detta uppdrag – det Nationella AI-uppdraget – har god AI-kompetens och erfarenheter från eget AI-arbete och initiativ. Vi ser redan idag att AI skapar tydliga nyttor inom enstaka förvaltningar samtidigt är det en bråkdel av den potentialen AI skulle ha för hela den offentliga förvaltningen. Vi ser att det saknas en övergripande samordning vilket gör att mycket dubbelarbete sker, att goda resultat inte sprids och att möjliga nyttor, skaldriftsfördelar med mera inte uppnås. I arbetet med uppdraget har det framkommit att det inom offentlig förvaltning finns en stor efterfrågan på allomfattande och konkret stöd i att ta fram AI-lösningar, säkra tekniska miljöer, att utveckla AI-tjänster i samt guidning och vägledningsmaterial. Detta gäller särskilt för mindre aktörer inom offentlig förvaltning som riskerar att helt eller delvis stå utan möjligheter att bidra till att uppnå nyttorna. Utan åtgärder är det vår uppfattning att skillnader mellan aktörer inom offentlig förvaltning kommer att öka eftersom AI ger stora fördelar för de som kan använda och utveckla AI.

Under våren 2023 är Sverige ordförande i Europeiska unionens råd. Samtidigt förhandlas AI-förordningen¹ som förväntas få stor påverkan på användningen av AI inom EU. Vår uppfattning är att svensk offentlig förvaltning som helhet kommer att bli kraftigt begränsade i sin möjlighet att använda AI om inte det

¹ Förslag till förordning om harmoniserade regler för artificiell intelligens och om ändring av vissa unionslagstiftningsakter (COM/2021/206 final)

finns en tydlig styrning och samordning för att förbereda offentlig förvaltning på den kommande förordningen.

I Sverige sker stora satsningar på forskning på AI inom näringslivet men liknande initiativ saknas inom offentlig förvaltning. Svensk offentlig förvaltning står på en stark grund men ska Sverige nå målet för AI-inriktningen och målen för digitaliseringspolitiken behöver regeringen investera för att vinster och nyttor ska nås.

Arbetet i uppdraget har resulterat i följande konkreta resultat:

- En samarbetsplattform där leveranserna från AI-uppdraget levereras; en AI-guide, förtroendemodell och information om relevanta AI-projekt. Resultaten har tillgängliggjorts publikt <https://offentligai.se> för att uppmuntra till lärande, delande och vidareutnyttjande inom offentlig förvaltning, akademi och näringsliv.
- Två AI-byggblock (en översättnings- och transkriberingstjänst) som enligt planen ska tillgängliggöras i Ena-strukturen.
- Ett policylabb tillsammans med deltagande myndigheterna, Combient AB och RISE Research Institutes of Sweden AB med syftet att undersöka hur kommande AI-förordning kan påverka AI-arbetet i praktiken.
- Behovsanalyser som visar på ett tydligt behov av en förvaltningsgemensam insats för att tillgängliggöra en AI-infrastruktur för alla offentliga aktörer i Sverige.

Dessa åtgärder är dock inte tillräckliga för att uppnå regeringens mål och för att främja AI inom offentlig förvaltning och kunna realisera de nyttor som finns med AI. Vi behöver göra mer. Därför rekommenderas i denna rapport ett fortsatt arbete i ett nytt regeringsuppdrag för att gå vidare med följande åtgärder:

- Ett fortsatt arbete för att tillgängliggöra en AI-infrastruktur som möjliggör utveckling av AI-drivna tjänster för alla aktörer inom offentlig förvaltning. Det blir möjligt för alla att på ett jämlikt sätt ute i landet och i de olika sektorerna experimentera och ta fram AI-lösningar med öppna eller egna data. En sådan infrastruktur innebär att fler aktörer inom offentlig förvaltning kan realisera AI-potentialen till en låg kostnad och i en säker och beprövad miljö. Detta inkluderar utredande aktiviteter för att säkerställa rätt nivå gällande bl.a. informationssäkerhet och vissa juridiska frågor. Vi ser behovet av säkra it-miljöer för svenska aktörer att verka i.

- Fortsatt utveckling av plattformen offentligai.se inklusive AI-guide, samling av exempel på användning av AI och öppen källkod och standardiserade dataset för AI.
- Vidareutveckling av förtroendemodellen för att bibehålla eller öka förtroendet för användningen av AI inom offentlig förvaltning inklusive utredning om förtroendemodellen i någon utsträckning ska vara tvingande att använda för offentlig sektor.
- Genomförande av policylabb för att förbereda för AI-förordningen.

Den sammanlagda kostnaden för detta är cirka 25 miljoner årligen till 2026 då uppdraget föreslås avslutas.

Fler myndigheter har uttryckt intresse att delta i en eventuell fortsättning och bör involveras i det fortsatta arbetet. Genom gemensamt arbete och tydliga satsningar på AI kan svenska invånare och företag få stora nyttor av AI. Bara genom att arbeta med policylabb i förberedelse för AI-förordningen bedömer vi att offentlig sektor kan spara 40 miljoner kronor. Kan offentlig förvaltning också gemensamt utveckla och tillgängliggöra en förvaltningsgemensam AI-infrastruktur som dessutom är tillgänglig för alla, istället för ett fåtal, sparar offentlig sektor enligt vårt räkneexempel 250 miljoner kronor eller mer.

Det finns stor potential att använda AI, den stora risken är att satsningarna uteblir och att svensk offentlig förvaltning hamnar längre efter vilket riskerar svensk välfärd och säkerhet.

Innehållsförteckning

Förord	1
Sammanfattning.....	2
1 Inledning	7
1.1 <i>Bakgrund och uppdrag</i>	7
1.2 <i>Metod och leveranser</i>	8
1.2.1 <i>Landningssidan offentligai.se</i>	9
1.3 <i>Avgränsningar och konsekvenser</i>	10
2 Arkitektur och infrastruktur	12
2.1 <i>Bakgrund och genomförande</i>	12
2.2 <i>Två byggblock som föreslås realiserar på kort sikt</i>	14
2.3 <i>På medellång sikt – ett fysiskt gemensamt träningskluster</i>	15
2.3.1 <i>Nyttor med ett fysiskt gemensamt träningskluster</i>	16
2.3.2 <i>Förutsättningar för leverans</i>	18
2.3.3 <i>Ett räkneexempel avseende etablering av ett fysiskt gemensamt träningskluster</i> 19	
3 Förtroendemodell	21
3.1 <i>Bakgrund och genomförande</i>	21
3.2 <i>Avvägningar</i>	22
3.3 <i>Slutsatser</i>	23
4 AI-guiden.....	25
5 Tillhandahålla information om relevanta AI-projekt.....	26
6 Policylabb.....	27
6.1 <i>Ett räkneexempel avseende nyttor för ett policylabb</i>	27
7 Slutsatser och rekommendationer	29
7.1 <i>Stort behov av stöd, kompetens, samordning och myndighetsgemensamt arbete</i>	29
7.2 <i>Rekommendationer</i>	30
7.3 <i>Kostnadsbedömning avseende förslaget fortsatt uppdrag</i>	32
8 Litteratur och inspirationsförteckning	34
8.1 <i>Sakkunniga hos organisationer som bidragit till uppdragets genomförande</i>	34
8.2 <i>Förteckning över material som bidragit till uppdraget</i>	34

Bilaga 1 Policylabb och AI-förordningen37

1 Inledning

1.1 Bakgrund och uppdrag

Riksdagens digitaliseringspolitiska mål är att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter (prop. 2011/12:1, utg.omr.22, bet. 2011/12:TU1, rskr. 2011/12:87). I regeringens digitaliseringsstrategi För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi (N2017/03643) lyfts digital innovation fram som ett delmål. I den nationella inriktningen för AI har regeringen ställt upp målsättningen att Sverige även ska vara ledande i att tillvarata möjligheterna som användning av AI kan ge, med syfte att stärka både den svenska välfärden och den svenska konkurrenskraften (N2018/03008).

Det totala ekonomiska värdet av ett fullständigt införande av nuvarande AI teknik i svensk offentlig förvaltning beräknades år 2020 uppgå till cirka 140 miljarder kronor med den AI teknik som redan fanns tillgänglig 2020.² Då motsvarade det cirka 6 procent av totala offentliga utgifter. Av dessa 140 miljarder kronor tillfaller cirka 106 miljarder kronor offentlig verksamhet i form av högre produktivitet, ökade intäkter och minskade utbetalningar. Cirka 34 miljarder kronor tillkommer andra aktörer såsom företag och arbetstagare, som en direkt följd av åtgärder inom offentlig förvaltning. Därutöver bedöms det finnas indirekta ekonomiska värden som inte har kvantifierats samt ytterligare betydande sociala och kvalitativa värden i form av bättre livskvalitet, rättvisa och miljö med mera.

Teknikutvecklingen för AI går mycket snabbt. Lanseringarna av chatbotten Chat GPT och bildgenereringstjänsten Dalle-E framtaget av AI-forsknings- och distributionsföretaget Open AI är exempel på detta och visar hur kraftfull AI kan vara. Nya användningsområden för tekniken upptäcks löpande och dess socioekonomiska konsekvenser är näst intill omöjliga att förutse eller kvantifiera.

De ekonomiska nyttorna som har tidigare identifierats (och beskrivits ovan) återfinns främst inom tvärsektoriella tillämpningar såsom inom administrativa stödprocesser. Utöver sektoriella nyttor inom sjukvård, omsorg, utbildning och kultur så finns det stora vinningar att hämta hem från ärendehanteringssystem, matchning mellan behov och utbud (till exempel inom arbetsmarknadspolitiken), rättigheter och utbud (till exempel inom bistånd och välfärd) samt skyldigheter och krav (till exempel inom

² Se Främja den offentliga förvaltningens förmåga att använda AI, Delrapport i regeringsuppdraget I2019/01416/DF || I2019/01020/DF (delvis)

skatteförvaltning). Infrastruktur pekas även ofta ut som en delsektor med stor nyttopotential för AI-baserade system till exempel för prediktivt underhåll, men det finns även ett behov av en gemensam digital infrastruktur för att dessa nyttor ska kunna uppnås. Investerings- och omställningskostnaderna i form av parallella verksamheter och system samt bristande styrning och uppföljning gör att nyttor ofta inte realiserar. Detta tillstånd gäller för allmänt tillämpliga teknologier som internet, molnlösningar och i mycket stor grad för AI.

Regeringen anser att det är viktigt att lösningar och verktyg som utvecklas inom offentlig förvaltning kommer till nytta inom hela den offentliga förvaltningen. Mot denna bakgrund beslutade regeringen i juni 2021 att ge Arbetsförmedlingen, Bolagsverket, Digg och Skatteverket i uppdrag att främja offentlig förvaltnings användning av AI.

Denna rapport är återrapporteringen av uppdraget.

1.2 Metod och leveranser

Uppdraget har genomförts i samverkan mellan de fyra myndigheterna, men i vissa delar av projektet har ansvaret fördelats ut bland myndigheterna. Skatteverket har haft särskilt fokus på arbetet med den digitala AI-infrastrukturen, Arbetsförmedlingen för AI-guiden, Bolagsverket har arbetat med förtroendemodellen och Digg med information om relevanta AI-projekt och en landningssida för gemensamma resultat. I arbetet med infrastruktur, AI-guide och förtroendemodell har dock alla myndigheter deltagit.

Under hösten 2021 bildades en styrgrupp för uppdraget som fram till i september 2022 samlades en gång i veckan för ett kortare möte och senare under projektet på månadsbasis. Utöver dessa veckomöten har fyra längre halvdagsmöten hållits under genomförandet.

Varje vecka har vi genomfört informationsmöten dit alla som arbetar på någon av myndigheterna varit välkomna.

Av regeringsuppdraget framgår att myndigheterna ska ha ett nära samarbete och vid behov delta i relevanta AI-miljöer i Sverige. Vi skulle även samverka med relevanta aktörer inom myndigheter, regioner, kommuner, lärosäten, forskningsinstitut samt privat sektor.

Representanter från uppdraget har deltagit i ett antal sammanhang, dels för att informera om uppdraget, men även för att samverka med andra aktörer. Exempelvis deltog styrgruppen vid Myndigheternas AI-nätverk i mars 2022.

Representanter från uppdraget har vid ett flertal tillfällen haft dialog med andra aktörer exempelvis SKR:s AI-nätverk och återkommande möten med eSam och AI Sweden.

Av regeringsuppdraget framgår även fyra områden som uppdraget ska fokusera på, flera av dessa föreslogs i redovisningen av uppdraget Främja den offentliga förvaltningens förmåga att använda AI.³ Dessa är att:

- Komplettera den förvaltningsgemensamma digitala infrastrukturen Ena – Sveriges digitala infrastruktur med till exempel referensarkitektur för AI samt AI-tillämpningar och komponenter som fritt kan användas av offentliga aktörer
- Ta fram en AI-guide för offentlig förvaltning
- Vidareutveckla den förtroendemodell för automatiserat beslutsfattande med stöd av AI som Digg och Lantmäteriet tidigare tagit fram
- Tillhandahålla information om relevanta AI-projekt

Därtill ska deltagande myndigheter vid behov initiera eller delta i testbäddar och regulatoriska sandlådor. Myndigheterna ska undersöka möjligheten att delta i utlysningar gällande AI som finns inom ramen för EU-program samt delta i den arena för datadelning som upprättas i enlighet med uppdraget om att främja delning och nyttiggörande av data (I2021/01826).

1.2.1 Landningssidan offentligai.se

AI-guide, förtroendemodell och information om relevanta AI-projekt publiceras på samarbetsplattformen <https://beta.dataportal.se>. Leveranserna från AI-uppdraget samlas där under en egen sida (<https://beta.dataportal.se/offentliga>) som är sökbar och går att nå via URL:en <https://offentligai.se> från den 24 januari 2023. Offentligai.se blir därmed en integrerad del av den samarbetsplattform som upprättas i enlighet med uppdraget om att främja delning och nyttiggörande av data (I2021/01826). Resultaten har tillgängliggjorts publikt för att uppmuntra till lärande, delande och vidareutnyttjande inom offentlig förvaltning, akademi och näringsliv.

Samarbetsplattformen är en vidareutveckling av Sveriges dataportal. Under 2022 påbörjades utvecklingen mot att skapa plattformen som bidrar till samarbete kring gemensamma digitala resurser och därmed blir ett stöd i att främja offentliga och privata aktörers samverkan kring datadriven innovation och AI. Plattformen är unik i sitt slag; här hålls den nationella förteckningen för sökbara offentliga data⁴, ges möjlighet att utforska data och dela data, applikationsgränssnitt och källkod samt möjligheter till att utbyta erfarenheter och kunskap. Genom att AI-området blir en integrerad del i samverkansplattformen kan synergier uppnås genom nyttjande av den

³ Delrapport i regeringsuppdraget I2019/01416/DF || I2019/01020/DF (delvis)

⁴ Här avses den digitala förteckning över data som har gjorts tillgängliga eller sökbara på internet som anges i 2 kap. 6 § lagen (2022:818) om den offentliga sektorns tillgängliggörande av data som Digg har till uppgift att publicera

gemenskap som finns kring dataportalen med dess forum (eng. community), referensbibliotek, nyheter, sökfunktion, verktyg och andra digitala resurser kopplat till data och datadelning. Med integrationen undviks kostsam dubbelförvaltning av kod och funktionalitet.

Samarbetsplattformen bygger på en utvecklad federerad princip för 1) datadelning, 2) engagemang i forumet samt 3) innehållshantering. I dag är samarbetsplattformen lanserad i sin allra första fas, en s.k. betaversion. Plattformen är skalbar och erbjuder goda möjligheter till fortsatt vidareutveckling för att möta nya behov, förväntningar och för att följa med i utvecklingen AI-området. För att komma vidare med fortsatt utveckling och partnerskap krävs förstärkta medel, enligt de bedömningar som Digg tidigare gjort till exempel i redovisningen av uppdraget Främja den offentliga förvaltningens förmåga att använda AI⁵, i delrapportering av uppdraget att Främja delning och nyttiggörande av data⁶ samt i myndighetens budgetunderlag för år 2023–2025.

Den del av uppdraget som syftar till att utveckla den gemensamma digitala infrastrukturen finns delvis beskriven på landningssidan men även mer utförligt i den här rapporten under kapitel 2.

1.3 Avgränsningar och konsekvenser

Uppdraget har inte medfört några resultat som ger konsekvenser för företag. Flera företagsrepresentanter har dock uttryckt ett behov av en samlad källa för information och kontakter gällande AI för offentlig förvaltning. Genom att samla information och ge ut frivilliga ramverk som förtroendemodellen har företag lättare att förutse vad som behövs och krävs från offentlig förvaltning vilket underlättar möjligheten att skapa relevanta erbjudanden. Tillgång till en teknisk miljö med till exempel referensarkitektur, verktyg för utveckling av AI-drivna tjänster samt tillämpningar som alla ges ut med öppen källkod har lett till stort intresse då företag i sin tur kan vidareutveckla samt enklare får en förståelse för vad som görs inom offentlig förvaltning gällande AI.

En viktig faktor att nämna avseende offentlig förvaltnings infrastrukturer är att även om offentlig förvaltning i dagsläget behöver egna infrastrukturer, bör det över tid vara möjligt att köpa till exempel beräkningskraft eller lagringskapacitet från kommersiella aktörer i anslutning till de egna infrastrukturererna. Detta innebär alltså att offentlig sektor kommer att ha

⁵ Delrapport i regeringsuppdraget I2019/01416/DF || I2019/01020/DF (delvis)

⁶ <https://www.digg.se/download/18.6ed9951a183cbe10d8a15e/1665650709359/Delrapport-uppdrag-framja-delning-och-nyttiggorande-av-data.pdf>

behov av och möjlighet att skala upp utveckling och drift av AI-drivna tjänster till publika moln (så kallade hybridmoln) för de lösningar som kan ligga där.

Policylabbet som beskrivs i kapitel 6 är ett resultat av dialoger mellan deltagande myndigheter och företagsrepresentanter och svarar mot det behov som finns av att gemensamt inom offentlig förvaltning förbereda sig för AI-förordningen.

2 Arkitektur och infrastruktur

2.1 Bakgrund och genomförande

I Regeringsuppdraget uppdras myndigheterna att ”komplettera den förvaltningsgemensamma digitala infrastrukturen (Ena)⁷, med till exempel referensarkitektur för AI samt AI-tillämpningar och komponenter som fritt kan användas av offentliga aktörer”.

Utifrån formuleringen i regeringsuppdraget har vi tolkat den önskade leveransen som utredning och leverans av s.k. AI-byggblock.⁸ Dessa ska ingå i den etablerade Ena-strukturen.

För att identifiera behov och möjligheter med olika AI-byggblock har ett explorativt arbetsätt använts. Arbetet inleddes med att ta fram en definition av vad ett AI-byggblock är.

Definition – AI-byggblock

AI-drivna tjänster som kan delas och tillgängliggörs fritt för aktörer i offentlig förvaltning

AI-infrastruktur som tillhandahålls av en myndighet till andra offentliga aktörer

Konceptuella modeller, kod eller instruktioner för lösning av specifika utmaningar i användning av AI hos offentliga aktörer

Övergripande referensarkitektur för AI

Bild 1: AI-uppdragets definition av ett AI-byggblock.

Utifrån denna definition identifierades möjliga AI-byggblock som skulle kunna tillhandahållas av de myndigheter som ingick i uppdraget.

Dessa byggblock testades sedan i behovsanalyser gemensamt med andra myndigheter, regioner och kommuner samt aktörer såsom eSam, Sveriges Kommuner och Regioners AI-nätverk och AI Sweden. I behovsanalyserna

⁷ Sedan uppdraget gavs har den infrastruktur som utvecklas enligt regeringsuppdragen I2020/03366 och I2020/02753 getts namnet Ena – Sveriges digitala infrastruktur.

⁸ För Ena:s definition av byggblock se: <https://www.digg.se/ledning-och-samordning/ena---sveriges-digitala-infrastruktur>

framkom att det finns en stor potentiell nytta i att samlas kring att utveckla olika AI-byggblock för offentlig förvaltning.

Bilden visar alla de byggblock som identifierats vid workshops och som har använts som grund vid behovsanalyserna. De grönmarkerade byggblocken är de som identifierats som de första som föreslås utvecklas beroende på behovsgrad men också genomförbarhet. Vi återkommer senare i rapporten främst till de grönmarkerade byggblocken.

Möjliga gemensamma AI-byggblock



Bild 2: Möjliga gemensamma AI-byggblock

Behoven av AI-byggblock konstateras vara väldigt olika beroende på vilken aktör som tillfrågas. Nästan alla aktörer säger sig ha stort behov av en förvaltningsgemensam teknisk AI-infrastruktur, samtidigt som några behöver stöd och tillgång till färdiga tjänster som kan delas och användas fritt på olika sätt. Färdiga, eller delvis färdiga, tjänster och modeller kan tillgängliggöras som en e-tjänst som kan anropas för att leverera ett resultat eller i tillämpliga fall som nedladdningsbar tjänst för användning i egen miljö.

Sammanfattningsvis fanns det en stark efterfrågan av gemensamma AI-byggblock på samtliga nivåer.

Det har också framkommit att det finns juridiska utmaningar som bland annat rör möjligheten att dela data, dela källkod, gemensamt träna, utveckla och dela färdiga tjänster.

Utifrån de behovsanalys som genomförts och de givna förutsättningarna för uppdraget har vi delat upp möjligheterna till realisering av de grönmarkerade byggblocken i två faser; byggblock som kan realiseras på kort sikt och ett byggblock som kan realiseras på medellång sikt.

Prioriteringen har gjorts utifrån de möjligheter och begränsningar som finns vad gäller framför allt tillgängliga data och tjänster, kompetens och rättsliga förutsättningar. De byggblock som föreslås är genomförbara med hänsyn till ovan nämnda faktorer.

Som nämndes i inledningen finns ett antal möjliga byggblock som inte utretts vidare i innevarande uppdrag. Bedömningen från behovsanalyserna är dock att det finns stor potential i flera av dessa.

På bild 2 ovan visas även de byggblock som identifierats men ännu inte prioriterats eller bedömts som kortsiktigt genomförbara (grönmarkerats). I ett fortsatt uppdrag skulle vidare utforskning av även dessa kunna ske

2.2 Två byggblock som föreslås realiseras på kort sikt

Två AI-drivna tjänster har valts ut som de första att utredas vidare för att kunna ingå i Ena. De är:

- En *översättningstjänst* för offentliga aktörer - publicerad via ett API⁹
- En *transkriberingstjänst* för offentliga aktörer - publicerad via ett API

När dessa AI-tillämpningar finns färdiga kan en offentlig aktör skicka in en text till översättningstjänsten eller en ljudfil till transkriberingstjänsten via ett API. En översatt text på något av de valda språken eller en transkriberad text på svenska blir då producerad och skickas tillbaka. Dessa är relativt enkla AI-drivna tjänster med hög genomförbarhetsgrad. Många offentliga aktörer signalerar behov av dessa då de skulle skapa stor nytta i vardagen, eftersom skyddsvärd information inom offentlig förvaltning effektivt och säkert kan översättas och transkriberas.

Det bör också ges möjlighet att ladda ned tjänsterna till egen driftsmiljö för att anpassa och använda tjänsterna i sin egen verksamhet. Tjänsterna bör i hög grad bygga på öppen källkod och öppna standarder för att fritt kunna tillgängliggöras till offentliga aktörer. Dock behöver grafiska användargränssnitt, användarvillkor, SLA, autentiserings- och auktorisationstjänster etcetera utvecklas och formuleras så att alla aktörer kan ansluta sig. Utvecklingen av de senare är beroende av hur andra byggblock i Ena kan användas.

Samtliga myndigheter som ingår i AI-uppdraget ingår också i Ena-samarbetet. Vid uppdragets redovisning finns en till ENA inskickad idéskiss som är det första steget i att ta dessa två tjänster in i ENA-strukturen. Planering för detta pågår vid denna rapportens inlämnande i det taktiska samordningsforumet för Ena. På

⁹ Eng. application programming interface eller applikationsprogrammeringsgränssnitt.

nästa möte ska förslagen lyftas för beslut om att gå vidare i utforskande utveckling, där bland annat nyttor och rättsliga förutsättningar utforskas (första utvecklingssteget i byggblocksarbete). Om arbetet drivs vidare beror på om myndigheterna har resurser för arbetet och om de sakanslag som finns för arbetet med Ena kan användas.

Vid inlämnandet av denna rapport är det oklart om budgeten som finns för byggblock i ENA räcker till finansiering av dessa nya AI-byggblock. Kostnaden för att vidareutveckla, tillgängliggöra samt förvalta de två byggblocken är rapporterade till ENA och kostnaden redovisas även här.

- Kostnad för vidareutveckling och tillgängliggörande beräknas till 2,1 miljoner kronor.
- Årlig kostnad för förvaltning beräknas till 1,4 miljoner kronor.
- En årlig vidareutveckling avseende modeller samt tjänster beräknas till 600 000 kronor.

Ovanstående kostnadsestimeringar gäller båda tjänsterna.

2.3 På medellång sikt – ett fysiskt gemensamt träningskluster

I arbetet med att identifiera möjliga AI-byggblock har det tydligt framkommit att offentliga aktörer i Sverige behöver en gemensam infrastruktur för träning och utveckling av AI-drivna tjänster. En sådan "träninginfrastruktur" innebär att offentliga aktörer kan få tillgång till en säker digital yta i en förvaltningsgemensam AI-infrastruktur där de själva, och i tillämpliga fall tillsammans med andra, kan bygga och testa AI-drivna tjänster och modeller med egna eller öppna data. I de fall det är tillåtet kan aktörerna också dela data och/eller modeller med varandra. I dag saknas för många, särskilt mindre, aktörer inom offentlig förvaltning, en skyddad och säker digital miljö som lever upp till säkerhetskrav, rättsliga krav och hållbarhetskrav som omgärdar AI i offentlig förvaltning.

På sikt kan en sådan träningsinfrastruktur också kompletteras med ytterligare ett byggblock för produktionssättning av färdiga AI-drivna tjänster för de offentliga aktörer som behöver det.

En skalbar AI-infrastruktur med stora delar av de egenskaper vi tänker oss i detta AI-byggblock finns redan i drift på Skatteverket i två olika infrastrukturkluster; ett för träning och utveckling och ett annat för produktionssättning av färdiga AI-tjänster. Dessa miljöer består till stora delar av komponenter med s.k. öppen källkod vilket gjort det enklare att anpassa lösningarna så att de bättre uppfyller kraven som offentlig förvaltning måste uppfylla i anslutning till utveckling av AI-drivna tjänster. Det gör det också enklare att fritt tillgängliggöra dem till andra offentliga aktörer. I ett tillgängliggörande skulle även vissa kommersiella produkter kunna ingå.

Skatteverket har utvecklat och använder själva denna tjänst idag samt levererar grunden till Kronofogdemyndigheten och Valmyndigheten. Skatteverkets miljöer är skalbara och kan tillsammans med övriga aktörer i uppdraget kopieras, skalas upp, anpassas samt vidareutvecklas så att de fungerar som infrastruktur för alla offentliga aktörer. Vi föreslår nu att investeringarna som är gjorda hos Skatteverket samt hos andra myndigheter konsolideras och återanvänds i ett gemensamt träningskluster som tillgängliggörs för alla offentliga aktörer i Sverige.

Vi ser därmed behov av ett fortsatt gemensamt regeringsuppdrag under kommande år för att förbereda för att implementera ett sådant AI-byggblock. Samspelet med andra aktörer är mycket viktigt för att få full effekt av arbetet som under 2023 skall skapa förutsättningar för en tänkt leverans av en förvaltningsgemensam AI-infrastruktur under 2024.

2.3.1 Nyttor med ett fysiskt gemensamt träningskluster

Ett antal nyttor för offentlig förvaltning och offentliga aktörer har identifierats avseende att leverera nämnda gemensamma AI-infrastruktur till alla delar av den svenska offentliga förvaltningen.

Dessa nyttor stärks bland annat av slutbetänkandet för utredningen ”Säker och kostnadseffektiv it-drift – förslag till varaktiga former för samordnad statlig it-drift”, (SOU 2021:97)¹⁰. Slutbetänkandet pekar på ett antal generella nyttor för offentliga aktörer genom att samexistera i gemensamma infrastrukturer. Noteras kan att slutbetänkandet egentligen avser endast statliga aktörer. Många nyttor som beskrivs i driftsutredningen kan dock bedömas vara direkt överförbara på offentliga aktörer i allmänhet. Slutbetänkandet innehåller också omfattande underlag för våra föreslagna aktiviteter avseende att skapa förutsättningar för en förvaltningsgemensam AI-infrastruktur. Nedanstående punkter är ett urval av nyttor som är direkt kopplade till en gemensam AI-infrastruktur för offentliga aktörer.

- Ett gemensamt träningskluster skulle påtagligt bidra till att uppfylla regeringens digitaliseringsmål samt beräknade effekthemtagningar som beskrivs i tidigare uppdrag¹¹, vilket gynnar offentlig förvaltning generellt och bidrar till att säkra välfärden. Detta genom att förslaget skapar förutsättningar för att under 2024 tillgängliggöra en avancerad, robust och säker AI-infrastruktur för utveckling och träning av AI-drivna tjänster för alla offentliga aktörer. Detta inkluderar även små och

¹⁰ <https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2021/12/sou-202197/>

¹¹ <https://www.digg.se/analys-och-uppfoljning/publikationer/publikationer/2020-01-14-framja-den-offentliga-forvaltningens-formaga-att-anvanda-ai>

medelstora aktörer som sannolikt inte skulle ha möjlighet att utveckla liknande AI-drivna tjänster på egen hand.

- Stora besparingar kan uppnås genom att dra nytta av de investeringar och ansträngningar som redan gjorts inom offentlig förvaltning vad avser utveckling av AI-infrastrukturer. Investeringarna har varit kostsamma samt resurs- och kompetenskrävande och nu är det möjligt att återanvända investeringarna så att de kommer hela offentlig förvaltning till gagn. Ingen detaljerad ekonomisk analys har skett inom ramen för innevarande uppdrag, men kostnaden för enskilda myndigheter att göra motsvarande insatser skulle vara omfattande. Genom att konsolidera utvecklingen på detta sätt kommer alternativa samhällskostnaden bli väsentligt lägre enligt våra övergripande beräkningar (se räkneexempel nedan under kapitlet Räkneexempel avseende etablering av ett fysiskt gemensamt träningskluster).
- Med en gemensam AI-infrastruktur för offentliga aktörer skapas förutsättningar för bättre kunna möta alla de krav som offentlig förvaltning måste leva upp till avseende bl.a. dataskydd-och sekretess, förvaltningsrättslig och liknande reglering samt hållbarhetskrav med mera. Dagens produkter på marknaden på AI-området är ofta relativt omogna i detta avseende och uppfyller inte kraven för offentlig förvaltning. Detta innefattar såväl befintliga som tillkommande krav i bland annat den kommande AI-förordningen. Om vi återanvänder investeringarna som gjorts för befintliga anpassade lösningar för ett gemensamt träningskluster för myndigheter, tillgodoses dessa grundläggande krav på ett effektivt och mer enhetligt sätt.
- Med en gemensam AI-infrastruktur som den föreslagna får vi en enhetlig och hög nivå av informations- och cybersäkerhet för de offentliga aktörerna på ett mer beprövat och effektivt sätt¹². I ett scenario där olika offentliga aktörer själva köper eller bygger infrastrukturer är det sannolikt att nivåerna kommer att skilja sig åt vilket kan innebära informations- och säkerhetsmässiga risker.
- Genom etablering av en gemensam AI-infrastruktur skapas en arena för gemensam kunskapsuppbyggnad och kompetensförsörjning på sikt. I en verklig och för offentliga aktörer praktiskt användbar miljö där verkliga data och komponenter som uppfyller kraven för offentliga aktörer kan

¹² Den föreslagna infrastrukturen är i de tidigare leveranserna väl beprövad och används redan idag för utveckling, test och produktion av kritiska tjänster. Till exempel kördes valsystemet i 2022 års val i en likadan infrastruktur och stod emot otaliga attacker under valnatten och därefter. (Den infrastrukturen innehåller inte AI förmågorna men är i grunden likadan).

användas blir ett samspel runt kompetens möjlig. Detta är också ett samspel som med hög sannolikhet ökar innovationsviljan hos våra offentliga aktörer.

- En gemensam AI-infrastruktur stödjer möjligheten att utföra experiment i verkliga förhållanden i anslutning till regulatoriska sandlådor i enlighet med den kommande AI-förordningen. Genom att etablera en gemensam infrastruktur är vi väl förberedda på den delen av införandet av AI-förordningen och kan därmed i tidigt skede utnyttja fördelarna med en sådan experimentmöjlighet som bidrar till att utveckla och accelerera AI-kompetensen och AI-användningen i både offentlig och privat sektor. Detta bidrar i sig till tidigare nämnda effekthemtagningar.
- I anslutning till infrastrukturen blir det möjligt att skapa och samla metadata till stöd för uppföljning av utveckling och progress i användning av AI i offentlig förvaltning i Sverige. När vi väl kan följa progressen blir det också lättare att peka på uppnådda effekter samt göra nödvändiga prioriteringar och satsningar framåt.

2.3.2 Förutsättningar för leverans

Som AI-byggblock betraktat är ett gemensamt träningskluster en mer komplex tjänst att bygga och leverera och alla förutsättningar behöver sättas på plats. En större arkitektur behöver ritas upp baserat på befintliga mindre infrastrukturkluster. Avtalsfrågor behöver lösas, juridiska frågor behöver utredas vidare med mera. Myndigheterna i uppdraget har en bild över vilka förutsättningar som behöver skapas och i slutet av denna rapport kommer vi att framföra en rekommendation om ett fortsatt uppdrag.

Kostnaden för att etablera en förvaltningsgemensam digital infrastruktur för AI beräknas till 35–45 miljoner kronor. Det är en uppskattning utifrån dagens befintliga miljöer samt den beräknade merkostnaden för att tillgängliggöra en sådan lösning som ett förvaltningsgemensamt träningskluster med alla nödvändiga förmågor.

Realiseringen av detta byggblock förutsätter således finansiering och ett fortsatt uppdrag.

2.3.3 Ett räkneexempel avseende etablering av ett fysiskt gemensamt träningskluster

Följande räkneexempel är baserat på tidigare erfarenheter från tidigare rapporter samt redan genomförda uppbyggnader av infrastrukturer av olika slag.¹³

Anta att det främst är de större aktörerna som utan stöd i en gemensam infrastruktur på egen hand har resurser att kunna arbeta med utveckling av egna AI-drivna tjänster (i en inköpt eller på egen hand uppbyggd infrastruktur).

- Vi har 3 storstadskommuner och 23 större städer i Sverige. Ett antagande baserat på viss insyn i de kommunerna, är att de 10 största kommunerna har möjlighet att med egen kraft jobba med att utveckla egna AI-drivna tjänster.
- Vi har 21 regioner som alla har relativt stora verksamheter med många årsarbetskrafter i sin verksamhet. Vi antar här att samtliga regioner har viss kraft att jobba med att utveckla egna AI-drivna tjänster för att uppnå samhällets mål och förväntade effekter.
- Under regeringen finns det just nu 344 myndigheter. 14 av dessa har över 4000 årsarbetskrafter. Låt oss anta att dessa 14 borde kunna arbeta med AI-drivna tjänster på egen hand i egna infrastrukturer.

Utifrån dessa antaganden har vi alltså 45 offentliga aktörer som på egen hand borde kunna effektivisera och förbättra sin verksamhet med hjälp av AI-drivna tjänster.

Nedan använder vi dessa antaganden för att få fram en alternativkostnad, det vill säga besvara frågan: Vad kostar det att inte bygga ett gemensamt träningskluster?

Vi räknar med att de 45 aktörerna från våra antaganden skulle bygga upp egna infrastrukturer till en kostnad om minst 10 miljoner kronor, vilket innebär en kostnad på 450 miljoner kronor totalt. Detta bedöms, baserat på erfarenheter, vara lågt räknat och snittkostnaden kommer troligen att vara högre.

Ovan har vi i vår alternativkostnadsberäkning antagit att samtliga 45 aktörer skulle ansluta sig till ett gemensamt träningskluster, vilket i praktiken inte behöver vara fallet. Därför räknar vi på att endast 70 procent av de 45 offentliga aktörerna skulle ansluta sig till ett gemensamt träningskluster. Då kvarstår 31 aktörer som tillsammans skulle ha en alternativkostnad på 310

¹³

miljoner kronor (31*10 miljoner kronor). Det är den summa som enligt våra antaganden direkt kan ställas mot kostnaden för en gemensam AI-infrastruktur enligt den grova uppskattningen i föregående stycke.

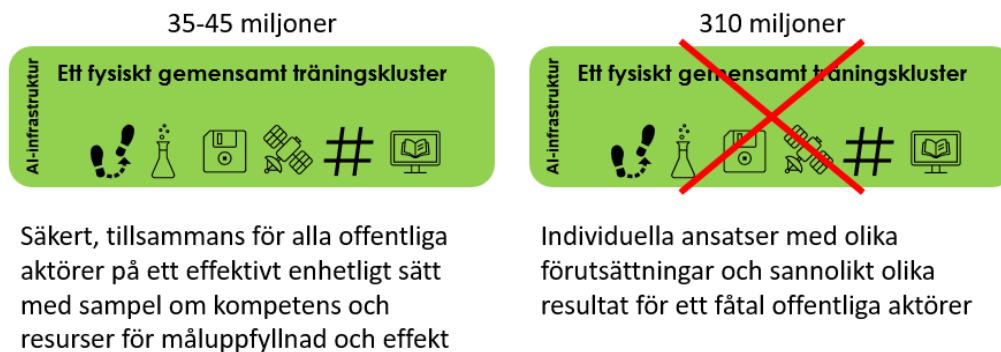


Bild 3: Skillnad mellan att utveckla tillsammans eller var för sig.

Givet dessa antaganden finns då fortfarande 330 myndigheter och 280 kommuner som har utmaningar att ta fram egna AI-drivna tjänster. Dessa kommer helt eller delvis att stå utanför möjligheterna till säker och hållbar effektivisering samt de förbättringar som AI-drivna tjänster kan bidra med i en organisation.

Ett antal av de i avsnitt 2.3.1 uppräknade nyttorna skulle inte heller uppstå om enskilda organisationer bygger eller köper egna infrastrukturer. Kvalitet, säkerhet, kravuppfyllnad och stöd för utveckling och hållbarhetsfaktorer skulle med stor sannolikhet divergera påtagligt. Synergier skulle inte heller uppstå i samma utsträckning och kompetensbristen i området skulle kunna göra att marknaden med stor sannolikhet inte skulle kunna täcka behovet. De slutliga kostnaderna för att offentliga aktörer på egen hand skulle klara dessa utmaningar skulle bli mycket höga för offentlig förvaltning i Sverige samt att nyttorealiseringsgraden skulle utebli.

3 Förtroendemodell

3.1 Bakgrund och genomförande

Förtroendemodellen, som tagits fram i ett första steg i ett tidigare regeringsuppdrag¹⁴, ska enligt föreliggande regeringsuppdrag vidareutvecklas för att kunna användas som ett frivilligt ramverk för offentlig förvaltning. I arbetet har Lantmäteriet deltagit på samma sätt som de fyra myndigheter som tilldelats regeringsuppdraget och i detta avsnitt avses med myndigheterna därmed även Lantmäteriet.

Den första iterationen av förtroendemodellen var i ett internationellt perspektiv ett av de första försöken att skapa en modell för att öka transparens i utvecklingen och användningen av AI, för att bibehålla eller öka förtroende för offentlig förvaltning. Modellen fokuserade på de tekniska delarna av användningen av AI och en slutsats var att modellen behövde utvecklas vidare.

Myndigheterna har arbetat på två sätt för att vidareutveckla modellen. Det ena sättet är att testa modellen på riktiga tillämpningar av AI-system internt och att utveckla den efter iterationer samt att låta externa testa modellen samt vara med i arbetet med att utveckla den. Det andra sättet har varit att använda omvärldsbevakning och dialoger nationellt och internationellt för att utveckla modellen, bland annat för att ta hänsyn till internationella rekommendationer och riktlinjer såsom UNESCO:s rekommendation om etisk AI.

Sedan den första modellen har flera arbeten vad gäller AI och transparens, tillsyn och AI i relation till olika sakområden gjorts i Sverige. Diskrimineringsombudsmannen och Jämställdhetsmyndigheten har bland annat tagit fram rapporter om hur deras områden kan påverkas av AI. Lärdomar från dessa arbeten har inarbetats i förtroendemodellen.

Internationellt har flera modeller som på olika sätt syftar till att motverka negativ bias, öka transparens och motverka diskriminering vid användning av AI tagits fram. Vi har utvärderat dem och i delar inspirerats men det har också blivit tydligt att det, såsom framgår i den svenska inriktningen för AI¹⁵, behövs en svensk modell som tar hänsyn till svenska förhållanden och regler för att modellen ska vara användbar.

Förtroendemodellen är uppdelad i tre delar. Den första delen är ett antal frågeställningar som varje myndighet bör reflektera över inför att verksamheten bestämmer sig för om AI kan vara en lösning för en utmaning

¹⁴ Uppdrag I2019/03237/DF om att testa ny teknik vid automatisering inom offentlig förvaltning.

¹⁵ Nationell inriktning för artificiell intelligens (N2018.14).

hos verksamheten. Den andra delen är det mest omfattande och är till för dem som bestämt sig för att använda sig av ett AI-system. Den tredje delen är ett kort som är till för uppföljning. Eftersom AI-system är beroende av data och ofta tränas med nya data kan AI-systemens resultat till exempel vad gäller träffsäkerhet kan förändras. Nya modeller som tillförs kan också påverka hur systemet agerar.

3.2 Avvägningar

Ett antal avvägningar har gjorts. Förtroendemodellen kan inte ta hand om alla omständigheter och bör inte vara för starkt styrande på detaljnivå eftersom varje verksamhet och sakområde är unikt. Att förtroendemodellen ska kunna användas av hela offentlig förvaltning gör också att modellen i hög utsträckning behöver vara generell.

Förtroendemodellen gör inte anspråk på att garantera ett ökat förtroende för en aktör som använder AI. Förtroende är mycket mer komplext än att använda sig av ett frivilligt ramverk eller en standard. Det är därför viktigt att förtroendemodellen inte ses som en enkel lösning för att lösa en större fråga. Ett utfall av detta ställningstagande är att förtroendemodellen ska vara ett verktyg för att systematisera och dokumentera och på så sätt själv utvärdera om verksamheten har förutsättningarna för AI på plats. Förtroendemodellen är därmed ett stöd och ingen garant för att aktörerna gjort allt rätt eller att förtroendet kommer att öka eller bibehållas utan andra åtgärder. Inte heller ger förtroendemodellen någon form av bedömning eller resultat, det kräver en mycket större organisation med bland annat tillsynsmöjligheter och modeller som är väldigt specifika för en verksamhet och en form av AI-system.

Utveckling av AI liknar i stort traditionell digital verksamhetsutveckling. Det innebär att mycket av den dokumentation och de hänsynstaganden som behöver göras ofta är sådana som en verksamhet är vana vid. Förtroendemodellen tjänar i det här avseendet främst till att uppmärksamma aktörer på sådant de behöver ta ställning till, till exempel att säkerställa rättslig grund för användningen av personuppgifter. Skillnaden gentemot traditionell it-utveckling ligger främst i användningen av data och mycket fokus ligger därmed på att underlätta för aktörer att ställa sig rätt frågor vad gäller användningen av data.

Vi har inte riktat in oss endast på automatiserade beslut som direkt träffar enskilda fattade av, eller med stöd av, ett AI-system utan förtroendemodellen ska även kunna tillämpas för AI-system på andra processer hos offentlig förvaltning. Förtroendemodellen kan användas som ett stöd vid upphandling av AI-system och till exempel kan ifyllandet av modellen på en adekvat nivå vara ett underlag i en upphandlingsprocess.

Utifrån den omvärldsanalys och de tester som gjorts för utvecklingen av förtroendemollen framgår det att det inte är givet att det är tillgång till mycket information som skapar eller bibehåller förtroende. Information om hur en AI-modell är uppbyggd är för de flesta kunskap som är svår att tillgodogöra sig. Däremot finns det i Sverige ett högt förtroende för myndigheter. En viktig aspekt för att upprätthålla förtroendet är fristående tillsynsmyndigheter som granskar andra myndigheter och garanterar att regler upprätthålls. Förtroendemodellen är därför också i stor utsträckning utformad för att möjliggöra en form av standard som ska underlätta för tillsynsmyndigheter, såsom Diskrimineringsmyndigheten eller Integritetsmyndigheten, att enkelt bedriva tillsyn av en myndighet som använt ett AI-system. Används förtroendemodellen vet tillsynsmyndigheten vad myndigheten bör kunna förvänta sig för typ av dokumentation.

Det har från flera myndigheter varit tydligt att de inte tror sig kunna ge ut all information i förtroendemodellen direkt till den som frågar, utan granskning av om till exempel sekretess gäller för någon del. Den ifyllda förtroendemodellen bör laddas hem till den lokala it-miljön hos verksamheten och hanteras enligt gängse regler för allmänna handlingar och utlämnande. Inte heller sparas någon information som fyllts i av den som gör förtroendemodellen på sidan för förtroendemodellen. Eftersom reglerna för allmänna handlingar och utlämnande gäller, möjliggör det för aktörer inom offentlig sektor att sekretessmarkera delar av förtroendemodellen när lagstöd för det finns.

Den som gjort en självutvärdering genom förtroendemodellen kan ladda hem en märkning. Märkningen kan visas upp på det sätt som passar myndigheten och är frivillig att använda. Märkningen kan utformas så att den länkar till sidan för förtroendemodellen så att den enskilda kan få mer information om förtroendemodellen. Syftet med detta är att öka förtroendet för användningen av AI eftersom den enskilda då ser att myndigheten har använt sig av en ordnad process vid utveckling av AI samt att märkningen underlättar för individer att använda sina rättigheter till att få mer information. När det gäller beslut riktade mot enskilda finns det också krav i allmänna dataskyddsförordningens artikel 22 som ställer krav på att det ska vara tydligt att AI använts när så är fallet. Liknande krav finns i artikel 56 i förslaget till AI-förordning.

3.3 Slutsatser

Utifrån det utåtriktade arbete som bedrivits för att inhämta synpunkter och kunskap uppfattar vi att det finns ett stort intresse av förtroendemodellen. Det är många aktörer som vill jobba med AI och som behöver stöd i vad aktörer behöver tänka på när de vill använda eller använder AI. Det verkar också finnas brister i systematisk dokumentation och att involvera olika kompetenser, såsom jurister och informationsspecialister, tidigt i utvecklingsprocesserna

med AI. Mycket av nyttan med förtroendemodellen, enligt våra erfarenheter, uppstår i dialogen som sker vid användningen av modellen.

En förtroendemodell möjliggör granskning och bevisföring och tillgängliggör information. Förtroendemodellen är ett första steg till att uppfylla en del av det som ses som grundläggande för automatisering i offentlig förvaltning och bidrar till ett ökat förtroende och tillit till offentlig förvaltnings nyttjande av AI.

För myndigheter som granskar andra myndigheter kommer förtroendemodellen kunna vara ett viktigt verktyg för att säkerställa adekvat användning av AI, vilket i sin tur bör leda till att allmänheten kan bibehålla eller till och med öka sitt förtroende för offentlig förvaltning när offentlig förvaltning i ökad utsträckning använder sig av AI.

Som stöd inför genomförandet av AI-förordningen kan förtroendemodellen också vara viktig. Vi upplever att det finns en stor oro över förordningen kommer att påverka möjligheten att använda AI, vilket även kan ses i de remissvar gällande AI-förordningen som inkommit till Regeringskansliet.¹⁶

Modellen behöver utifrån kommande beslut om AI-förordningen utvecklas. Utveckling behöver också ske utifrån synpunkter från användarna.

Det är inte otänkbart att förtroendemodellen kan utvecklas för att tjäna som en fri uppförandekod enligt art 69 i förslaget till AI-förordningen. I vissa länder, t.ex. Kanada, är det obligatoriskt för offentliga aktörer att använda deras motsvarighet till förtroendemodellen. I Finland finns liknande förslag¹⁷. För att möta behoven hos svensk offentlig förvaltning inom AI och för Sveriges möjlighet till påverkan av framtida uppförandekoder, standarder och ramverk är det enligt myndigheterna viktigt att vidareutveckla förtroendemodellen. Det är också relevant att utreda i vilken mån förtroendemodellen bör vara tvingande, för att garantera transparens och insyn i användningen av AI inom offentlig förvaltning.

¹⁶ I2021/01304

¹⁷ Diskrimineringsombudsmannens berättelse till riksdagen, 2022B 7/2022 rd

4 AI-guiden

AI-guiden tillgängliggörs via sidan offentligai.se. Det finns många olika sätt att arbeta med AI och varje organisation har sina egna behov och kompetenser. Med utgångspunkt i erfarenheterna från de fyra myndigheterna som arbetat med uppdraget beskrivs områden som är viktiga för aktörer som vill komma igång och utveckla sitt AI-arbete, med utgångspunkt i de områden som regeringen pekat i uppdraget.

Många offentliga aktörer har påbörjat verksamhetsutveckling med hjälp av AI men det är myndigheters uppfattning att det finns ett stort behov av stöd och kunskap, särskilt för mindre aktörer. Därtill finns ett behov av att kunna diskutera och fördjupa sin kunskap hos de aktörer som i dag använder AI.

Det finns därmed ett behov av att fortsätta utvecklingen av AI-guiden och särskilt av att samskapa via de möjligheter som offentligai.se ger. Utvecklingen går också fort, vilket ytterligare bidrar till behov av att utveckla och uppdatera innehållet samt ytterligare anpassa guiden utifrån offentliga aktörers behov.

5 Tillhandahålla information om relevanta AI-projekt

Att främja nyttjandet av AI inom offentlig förvaltning möjliggörs genom lanseringen av landningssidan offentligai.se. Den exempelsamling som publiceras där syftar till att ge aktörer som står inför utveckling eller implementering av en AI-baserad lösning i sin verksamhet, en djupgående inblick i andra offentliga aktörers erfarenheter av detta. Varje exempel har därför en egen sida där det går att ta del av information i form av en presentation i videoformat. Presentationen kompletteras med beskrivande text och information om personerna bakom projektet. Myndigheterna har aktivt säkerställt att exempel från kommunal, regional och statlig myndighetsnivå visas upp. Detta för att visa på bredd men också på skillnader. De exempel som lyfts fram behandlar inte enbart specifika tekniska lösningar utan belyser även organisationsfrågor, kompetensfrågor och datahanteringsfrågor.

Vi har fört dialog med aktörer i svenska AI-miljöer, som AI Sweden och eSam och aktivt samverkat för att undvika dubbelarbete när det gäller att visa på exempel på AI-tillämpningar. Vi har även undersökt möjligheten att samverka på EU-nivå för att visa upp svenska exempel men också för att inhämta exempel från andra länder. Även möjligheten till årlig uppföljning av hur AI användningen utvecklas utifrån sammanställning av användningsfall har undersökts. Dock har inte förutsättningarna funnits under uppdragets genomförandetid bland annat på grund av att den svenska landningssidan inte varit klar. Däremot kan detta utvecklas vid ett förlängt uppdrag.

Det finns även möjligheter att nyttja information från ifyllda förtroendemodeller för att följa upp och analysera nya AI-baserade projekt, utvecklingar och implementeringar. Detta möjliggör en löpande addering av användningsfall, med detaljerad beskrivning av olika aspekter av AI-baserade lösningar samt möjlighet att följa upp och analysera utvecklingen, lyfta fram trender och identifiera lösningar som potentiellt kan skalas upp. I nuläget sparas eller lagras ingen data som användare av förtroendemodellen fyller i men lösningar för att nyttja data från ifyllda modeller går att utveckla i samråd med slutanvändarna.

Under arbetet med att samla in goda exempel har det framkommit att det finns ett intresse från flera offentliga aktörer att även i framtiden kunna publicera nya projekt.

6 Policylab

Myndigheterna har tillsammans med Combient AB och RISE Research Institutes of Sweden AB inrättat ett policylab för att undersöka hur AI-förordningen kan påverka i praktiken. Policylabbet inrättades i oktober 2022 utifrån de tydliga behov som deltagande aktörer mötts av gällande förståelse av AI-förordningen.

I regeringsuppdraget har regeringen uppmanat till att vid behov initiera eller delta i testbäddar och regulatoriska sandlådor. Deltagande aktörer har valt att kalla formen för policylab då det saknas en gemensam lagstiftad definition av regulatorisk sandlåda både i Sverige och inom EU. Namnet är även valt för att förtydliga att det inte rör sig om en regulatorisk sandlåda som den som föreslås AI-förordningen då rättsliga förutsättningar för sådana saknas innan förordningen är beslutad. Någon möjlighet till testbädd har inte funnits även om det finns många behov av gemensamma miljöer för att utveckla AI.

Trots den korta tid som policylabbet varit igång har aktörerna redan kunnat identifiera flera gemensamma utmaningar och nyttor med arbetet. Vad som är tydligt är att AI-förordningen är komplicerad i sig, men också att AI-förordningen i förhållande till andra rättsakter, som till exempel förslaget till förordning om övergripande cybersäkerhetskrav för produkter med digitala element¹⁸, gör området än mer komplicerat.¹⁹ Komplexiteten riskerar att driva kostnader och riskera att minska användningen av AI och de nyttor som AI kan ge både för offentlig som privat sektor. Med policylabbet kan aktörerna göra analyser som kan vägleda svenska aktörer som vill använda AI vilket kommer reducera kostnader och möjliggöra för svenska aktörer att arbeta i överensstämmelse med AI-förordningen.

Vad gäller fortsatt utveckling av policylabbet bedöms det krävas fyra årsarbetskrafter, vilket motsvarar cirka 5 miljoner årligen.

6.1 Ett räkneexempel avseende nyttor för ett policylab

Fyrtiofem (45)²⁰ offentliga aktörer arbetar självständigt med att säkerställa att de lever upp till AI-förordningens krav. Två anställda per aktör arbetar med detta under ett år. Den genomsnittliga kostnaden för en årsarbetskraft i statlig

¹⁸ Förslag till förordning om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordning (EU) 2019/1020 (COM/2022/454 final)

¹⁹ Se bilaga 1

förvaltning är drygt en miljon kronor. Total kostnad för offentlig förvaltning blir 90 miljoner kronor för ett år.

Genom policy labbet kan gemensamma tolkningar, förberedelsematerial och guider tas fram. Kostnaden enligt ovan för detta är ca 5 miljoner per år. Samtidigt behöver varje verksamhet göra sin tolkning och bedömning samt kompetensutveckla sig. Arbetet antas minskas med hälften mot att börja från noll. Detta ger en sammanlagd nytta om 40 miljoner per år. Nyttan reduceras sannolikt årligen i och med att varje verksamhet bygger upp sin egen kompetens.

7 Slutsatser och rekommendationer

7.1 Stort behov av stöd, kompetens, samordning och myndighetsgemensamt arbete

Regeringen anser att det är viktigt att lösningar och verktyg som utvecklas inom offentlig förvaltning kan komma till nytta inom hela den offentliga förvaltningen. Som framgår inledningsvis och i vårt nuvarande arbete med AI finns stor potential för att skapa värde för offentlig förvaltning. Samtidigt finns flera utmaningar som bland annat består i kompetensbrist, tillgång till användbara data, kunskap om tillgänglig teknik, juridiska och etiska frågor. För att realisera de potentiella nyttorna med AI behöver Sverige komma tillrätta med och hantera utmaningarna. Genom att flera myndigheter samarbetar i utvecklingen av ramverk och AI-infrastrukturer ökar möjligheten för att realisera värden och potential till en lägre kostnad. Detta regeringsuppdrag är ett steg för att åstadkomma detta.

Vår bedömning är att utmaningarna är stora och behovet av samlat stöd har i viss mån överraskat oss. Utmärkande är det stora behovet av kompetens inom AI och då särskilt juridisk kompetens, men även kombinationen av kompetens att utveckla AI tillsammans med en förståelse för verksamheten. Eftersom kompetensen är svår att få och ofta spridd över många aktörer krävs ökad samverkan och samordning. Gemensamma miljöer för samverkan och för att sprida information behövs.

Vår bedömning är att det finns ett stort behov av ökad statlig styrning på AI-området för offentlig förvaltning. Även om varje verksamhet är unik har många liknande utmaningar och i dag sker mycket dubbelarbete som på samhällsnivå är kostsamt och ineffektivt. Ökad styrning mot förbättrad samordning är nödvändigt.²¹

Tydligt är att mindre (och även medelstora) aktörer inte har möjlighet att följa med i utvecklingen och att effektivitetsvinster därmed går förlorade. Därtill finns stora risker vad gäller cyberattacker och säkerhetsintrång när offentlig förvaltning inte samordnar sig. De större myndigheterna bör underlätta för

²¹ Vi stödjer oss i detta utöver våra egna bedömningar på bland annat slutsatserna från Säker och kostnadseffektiv it-drift – förslag till varaktiga former för samordnad statlig it-drift (SOU 2021:97), Förnya taktiken i takt med tekniken (SOU 2022:68) och Kraftsamling för ett hållbart digitaliserat Sverige (N2021/00041).

offentlig förvaltning genom att erbjuda miljöer som underlättar för vidareutveckling.

AI-förordningen kommer sannolikt att få stor påverkan på användningen av AI. Offentlig förvaltning behöver aktivt arbeta med att förbereda sig på förordningen och där kan bland annat policylabb ge ett stöd.

Ett resultat som inte är en direkt leverans är vikten av att arbeta med öppna data, öppen källkod och öppna standarder. Detta är något som vi identifierat som en möjliggörare för att ytterligare stärka användningen av AI. Inriktning på detta ger ökade möjligheter till att dela och utveckla gemensamt. Det ger också goda möjligheter för forskare att bedriva forskning samt för företag att vidareutveckla tjänster. Att arbeta med öppenhet bidrar till transparens vilket bidrar till tillit samtidigt som det bidrar till innovation.

7.2 Rekommendationer

Det övergripande syftet med rekommendationerna är att offentlig förvaltning ska vara väl rustad för att nyttja potentialen med AI samt öka användningen av AI utifrån målsättningen att Sverige ska bli ledande i världen på att använda AI. Detta kommer att bidra till mer effektiv och ändamålsenlig förvaltning med förbättrade resultat och större likvärdighet som följd.

Ökad kvalitet och effektivitet kommer att ha positiv inverkan på förtroendet för förvaltningen men även för AI-tekniken som sådan och digitaliseringen generellt. Genom samverkan och skapandet av gemensamma resurser i form av guider, praxis, infrastruktur och beräkningskapacitet med mera minskar dubbelarbetet och kostnaderna. En ökad förmåga och samsyn på teknikens möjligheter kommer även bidra till att bättre hantera samhällsutmaningar genom användning av digitala resurser inom bland annat välfärden.

Vi föreslår därför att vi tillsammans får ett förnyat uppdrag, med en löptid fram till 2026, för att fortsätta utveckla och förvalta landningssidan offentligai.se, AI-guide, exempelsamling och förtroendemodell. Året är valt utifrån att AI-förordningen då möjligen ska börja tillämpas men också för att en långsiktighet krävs för att stödet ska bli effektivt. På sikt kan utpekat ansvar för förvaltning av det som publiceras behöva utredas, men bland annat beroende på kompetensbristen och behovet av samordning bör alla myndigheterna, och möjligen fler, dela på ansvaret fram till 2026.

Gällande förtroendemodell anser vi att det i ett kommande uppdrag bör utredas i vilken utsträckning förtroendemodellen kan bli tvingande och hur ett system för tillsyn i så fall bör se ut.

Fortsatt arbete med policylabb bör också ingå i ett förnyat uppdrag, för att förbereda inför AI-förordningen. Resultat från policylabbet bör löpande publiceras via offentligai.se vilket kan bidra till stöd för hela offentlig

förvaltning men även för företag gällande förståelse av AI-förordningen. Detta går i linje med förslag som lämnats i slutbetänkandet *"Förnya taktiken i takt med tekniken"* (SOU 2022:68)²² om utvecklad samverkan mellan myndigheter för att använda och sprida kunskap om ny teknik. Samverkan med till exempel Integritetsskydds-myndigheten och Finansinspektionen vore positivt.

På sikt kan policylabbet utvecklas till en eller flera AI-regulatoriska sandlådor. Kan vi arbeta vidare med förslagen i denna rapport kan också policylabb integreras med den tekniska infrastrukturen som föreslås. Därigenom kan Sverige tidigt vara redo med både teknisk och administrativ infrastruktur och kunskap för att stötta svenska myndigheter och företag i användningen av AI enligt AI-förordningen. Vidare kan lärdomar från policylabb bidra till välinitierade svenska positioner i eventuella genomförandeakter för AI-förordningen.

Vi föreslår vidare att uppdraget inkluderar fortsatt arbete med en gemensam AI-infrastruktur. De byggblock som på kort sikt föreslås bli en del av Ena behöver få förutsättningar att fortsatta utredas och förhoppningsvis utvecklas och förvaltas.

De medel som idag finns avsatta för Ena är redan budgeterade 2023 för andra byggblock och grunddatadomäner. Det är möjligt att medel kan omprioriteras men det vet vi inte idag. Myndigheterna inom Ena har vid ett flertal tillfällen påpekat att ytterligare medel behövs för att kunna utveckla och förvalta den gemensamma infrastrukturen varför vår bedömning är att ytterligare medel behövs för att realisera de nyttor som AI-byggblocken kan ge.

I tillägg till att fortsätta arbetet med ovanstående byggblock bör det ramen för förslaget fortsatt uppdrag finnas ett deluppdrag med det tydliga målet att under 2023 konkret skapa förutsättningar för att under 2024 bygga ett fysiskt gemensamt träningskluster, innehållande förmågor för offentliga aktörer att träna och utveckla AI-drivna tjänster. Inriktningen bör vara att klustret och tjänsterna utvecklas och tillhandahålls med öppen källkod och standard i den utsträckning det är möjligt. En sådan miljö skulle påtagligt bidra till effektivisering och bättre förutsättningar för att förvalta och utveckla välfärden i Sverige. Ett sådant uppdrag bör delrapportera förberedelser för finansiering snarast möjligt samt i övrigt delrapporteras i slutet av 2023 med förslag på fortsatt utveckling och löpande finansiering.

Vidare är det av central vikt att det fortsatta regeringsuppdraget fokuserar på att förstärka och vidareutveckla strukturen rörande öppen källkod och öppna

²² Se särskilt. s. 140 ff.

data inom AI. Detta gör görs via offentlig.ai och dataportalen. Genom att samla, strukturera och tillgängliggöra dataset för AI kan fler aktörer lätt få tillgång till data för sin AI-utveckling. Detta arbete kompletterar gemensamma infrastrukturer.

Sammanfattningsvis rekommenderas ett fortsatt arbete i ett nytt regeringsuppdrag för att gå vidare med följande åtgärder:

- Ett fortsatt arbete för att tillgängliggöra en AI-infrastruktur som möjliggör utveckling av AI-drivna tjänster för alla aktörer inom offentlig förvaltning. Det blir möjligt för alla att på ett jämlikt sätt ute i landet och i de i olika sektorerna experimentera och ta fram AI-lösningar med öppna eller egna data. En sådan infrastruktur innebär att fler aktörer inom offentlig förvaltning kan realisera AI-potentialen till en låg kostnad och i en säker och beprövad miljö. Detta inkluderar utredande aktiviteter för att säkerställa rätt nivå gällande bland annat informationssäkerhet och vissa juridiska frågor. Vi ser behovet av säkra it-miljöer för svenska aktörer att verka i.
- Fortsatt utveckling av plattformen offentlig.ai inklusive AI-guide, samling av exempel på användning av AI och öppen källkod och standardiserade dataset för AI.
- Vidareutveckling av förtroendemodellen för att bibehålla eller öka förtroendet för användningen av AI inom offentlig förvaltning inklusive utredning om förtroendemodellen i någon utsträckning ska vara tvingande att använda för offentlig förvaltning.
- Genomförande av policylab för att förbereda för AI-förordningen.

7.3 Kostnadsbedömning avseende föreslaget fortsatta uppdrag

Vi bedömer att ett kommande uppdrag i enlighet med ovan kommer att kosta cirka 25 miljoner kronor årligen som fördelas i enlighet med:

- För att samordna, administrera och koordinera kommande uppdrag bedömer vi att det behövs två årsarbetskrafter, vilket motsvarar cirka 2,5 miljoner kronor.
- Fortsatt utveckling av offentlig.ai och de tjänster som över tid behöver vidareutvecklas inklusive AI-guide och förtroendemodell bedöms tre årsarbetskrafter krävas, vilket motsvarar cirka 4 miljoner kronor årligen. Däröver bedöms 1 miljon behövas för förvaltning, support och drift av själva landningsytan.
- För utveckling av policylabbet bedöms det krävas fyra årsarbetskrafter, vilket motsvarar cirka 5 miljoner årligen. Här finns stora vinster att hämta, vilket redovisats i kapitel 6.

- Kostnadsberäkning för de två första byggblocken som vid denna rapportts färdigställande är på väg in i ENA, transkribering- och översättningstjänst är som följer och gäller båda tjänsterna.
 - Kostnad för utforskande utveckling och tillgängliggörande beräknas till 2,1 miljoner kronor.
 - Årlig kostnad för förvaltning beräknas till 1,4 miljoner kronor.
 - En årlig vidareutveckling avseende modeller samt tjänster beräknas till 600 000 kronor.
- Aktiviteterna med syfte att under 2023 skapa förutsättningar för en eventuell byggnation av en förvaltningsgemensam infrastruktur under 2024 bedöms ta ca 5,5 miljoner i anspråk från myndigheterna under 2023, vilket bör finansieras genom föreslaget fortsatt uppdrag.
- Vad gäller arbetet med öppen källkod och öppna data som bör vidareutvecklas och integreras med befintliga plattformar, där dataportalen och offentlig.ai är centrala, bedöms tre årsarbetskrafter krävas, vilket motsvarar cirka 4 miljoner kronor årligen.

8 Litteratur och inspirationsförteckning

Följande förteckning avser kontakter och möten, källor, litteratur och artikelstudier samt inspirationskällor som bidragit till genomförandet av uppdraget.

8.1 Sakkunniga hos organisationer som bidragit till uppdragets genomförande

AI Sweden, Combient, Diskrimineringsombudsmannen, Domstolsverket, eSAM, Lantmäteriet, Jämställdhetsmyndigheten, EuroCC National Competence Centre Sweden, Region Halland, Region Skåne, Region Stockholm, Region Västra Götaland, Region Västerbotten, Research Institutes of Sweden (RISE), Riksarkivet, Statskontoret, Region Stockholm, Skellefteå kommun, Strängnäs kommun, Statistiska Centralbyrån, Örebro kommun.

För utvecklingen av förtroendemodellen har sakkunniga från Diskrimineringsombudsmannen, Göteborgs universitet, Integritetsskyddsmyndigheten, Jämställdhetsmyndigheten, Linköpings universitet, Lunds universitet, Statskontoret, Södertörns Högskola, Region Stockholm särskilt bidragit.

8.2 Förteckning över material som bidragit till uppdraget

A guide to using artificial intelligence in the public sector, The Government Digital Service UK.

Unescos recommendation om etik och artificiell intelligens, Unesco.

OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449.

The Dstl Discuit Book, DSTL/PUB115968, Ministry of Defence.

Etiska riktlinjer för tillförlitlig AI, Kommissionens expertgrupp på hög nivå för AI-frågor juni 2018.

Främja den offentliga förvaltningens förmåga att använda AI. Delrapport i regeringsuppdraget I2019/01416/DF och I2019/01020/DF (delvis).

Testa ny teknik för automatisering inom offentlig förvaltning I2019/03237/DF.

Säker och kostnadseffektiv it-drift – förslag till varaktiga former för samordnad statlig it-drift, SOU 2021:97-

Styrning och finansiering av förvaltningsgemensam digital infrastruktur, ESV 2020:23.

Den statliga värdegrunden – gemensamma principer för en god förvaltning, Statskontoret 2019.

Artificiell intelligens och jämställdhet, Jämställdhetsmyndigheten 2020.

Transparens, träning och data Myndigheters användning av AI och automatiserat beslutsfattande samt kunskap om risker för diskriminering, Diskrimineringsombudsmannen Rapport 2022:1.

Artificiell intelligens (AI) i Sverige 2019, Statskontoret.

Artificiell intelligens i svenskt näringsliv och samhälle, Vinnova VR 2018:08.

Artificiell intelligens i den offentliga sektorn - Hur 213 offentliga organisationer drar nytta av AI Europeiska utsikter för 2020 och framåt, EY och Microsoft.

Svenska folket och AI – Svenska folkets attityder till Artificiell Intelligens 2022, Bolagsverket Lunds universitet, Postnord, Göteborgs universitet, Insight Intelligence.

Varför AI? - Förutsättningar, möjligheter och hinder för företag att använda AI, Tillväxtanalys Rapport 2022:11.

Drivkrafter för ökad användning av AI, Tillväxtanalys Rapport 2021:07.

Juridik vid användningen av AI, eSAM, ES2022-08.

Suing the algorithm: the mundanization of automated decision-making in public services through litigation, Kaun Anne 2022.

Algorithmic resistance: Media practices and the politics of repair, Anne Kaun, Julia Velkova 2021.

Fostering the data welfare state: A Nordic perspective on datafication, Andreassen, Rikke, Kaun, A

Defining and Undefined Automated Decision-Making research: towards a people-centered approach (under utvärdering) Stine Lomborg, Anne Kaun, Sne Scott Hansen.

Automating Public Administration: Citizens' Experiences with Automated Decision-Making Across Three Welfare Regimes (Under utvärdering), Anne Kaun, Anders O. Larsson & Anu Masso.

Achieving a Data-Driven Risk Assessment Methodology for Ethical AI, Felländer, A., Rebane, J., Larsson, S., Wiggberg, M. & Heintz, F., 2022.

AI and Patients' Rights: Transparency and information flows as situated principles in public health care, Högberg, C. & Larsson, S., 2022.

Three Levels of AI Transparency, Haresamudram, K., Larsson, S. & Heintz, F., 2022.

AI in the EU: Ethical Guidelines as a Governance Tool, Larsson, S., 2021.

Tillit i den datadrivna handeln, Larsson, S. & Vetter, R., 2021.

Tillit eller tvång? Konsumenters förtroende för handelns datainsamling, Larsson, S., Emanuelsson, T. & Thiringer, S., 2020.

Transparency in artificial intelligence, Larsson, S. & Heintz, F., 2020.

Superintelligent socialtjänst? Gabriella Scaramuzzino, 2022.

Promoting equality in the use of Artificial Intelligence – an assessment framework for non-discriminatory AI, Atte Ojanen, Anna Björk, Johannes Mikkonen Demos Helsinki

X-RAI: A Framework for the Transparent, Responsible, and Accurate Use of Machine Learning in the Public Sector, Per Rådberg Nagbøl, Oliver Müller

Algorithmic Impact Assessment tool, Government of Canada.

Self-assessment guide for artificial intelligence (AI) systems, Commission Nationale de l'Informatique et des Libertés (CNIL).

Guidance on the AI auditing framework - Draft guidance for consultation, Information Commissioner's Office 2020.

Bilaga 1 Policylabb och AI-förordningen



Datum	Beteckning	Sida
2023-01-17	Policylabb inom uppdrag I2021/01825	37 (43)

Analys av myndighetsgemensamma AI-tjänster utifrån kommande EU-förordningar inom det Digitala årtiondet

Håkan Burden och Susanne Stenberg, RISE Research Institutes of Sweden

Analysen har gjorts i samarbete med Arbetsförmedlingen, Bolagsverket, Myndigheten för digital förvaltning och Skatteverket inom ramen för det gemensamma policy labbet som upprättats med anledning av regeringsuppdraget Uppdrag att främja offentlig förvaltnings förmåga att använda artificiell intelligens (I2021/01825).

Motivation och bakgrund

2021 gav den dåvarande regeringen Arbetsförmedlingen, Bolagsverket, Digg och Skatteverket uppdraget att främja offentlig förvaltnings förmåga att använda AI i syfte att stärka Sveriges välfärd och konkurrenskraft. Som ett delresultat av uppdraget har de fyra myndigheterna identifierat två AI-tjänster med potential att bli myndighetsöverskridande:

- 1) Identifiering för åtkomst till myndighetstjänster
- 2) Översättning av myndighetstjänster från svenska till ett eller flera språk

I det här dokumentet ger vi en översikt av hur de föreslagna tjänsterna relaterar till EU:s AI-förordning som föreslogs våren 2021 som en del av det digitala årtiondet. Sedan förordningen föreslagits har den genomgått stora förändringar under tre olika ordförandeskap. För att analysen ska vara relevant

har vi därför utgått från den version som ministerrådet antog i december 2022 inför förhandlingarna med parlamentet²³.

Eftersom uppdraget ska främja offentlig förvaltnings förmåga att använda AI och stärka svensk konkurrenskraft är det motiverat att se hur de föreslagna tjänsterna påverkas av kommande EU-regleringar och hur svensk förvaltning kan rusta sig inför nya uppdrag och ansvar i relation till kommande EU-regleringar.

Beskrivning av tjänsterna

Den första tjänsten berör identifiering för åtkomst till myndighetstjänster som ett alternativ till exempel Bank-ID. Tjänsten är tänkt att delas mellan flera myndigheter för att möjliggöra en identifieringstjänst mot svenska myndigheter. Den identifierade är att se som en aktiv part i identifieringen, något som är viktigt när tjänsten ska risk-klassificeras. En fördel gentemot existerande lösningar är att tjänsten utvecklas och förvaltas av svenska myndigheter och inte av privata aktörer.

Den andra tjänsten är en språkmodell för översättning. Det är vanligt att myndigheter får ta emot material på andra språk än svenska som underlag för beslut. Istället för att skicka materialet till en manuell tolktjänst kan det i vissa fall vara tillräckligt med en automatisk översättning. På så sätt kan ledtiderna kortas vilket påverkar handläggningstiden positivt. Förvaltningen ska fortfarande vara objektiv och rättssäker så beslut baserade utifrån automatiska översättningar kommer fortfarande behöva kvalitetssäkras. En fördel med automatiserade översättningar är att de kan harmoniseras så att översättningen av betydelsefulla koncept inte beror på översättaren utan alltid följer riktlinjerna för käll- och målspråken.

Klassificering av risk

Begreppet identifiering ingår i biometrisk fjärridentifiering vilket kommer regleras av AI-förordningen. Biometrisk fjärridentifiering kommer förbjudas om ändamålet är brottsbekämpning i offentliga miljöer även om det finns undantagsmöjligheter (artikel 5). Enligt definitionen är en förutsättning för fjärridentifiering att den identifierade inte är aktivt inblandad i processen

²³ Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - General approach, Brussels 25th November 2022: <https://artificialintelligenceact.eu/wp-content/uploads/2022/12/AIA—CZ—General-Approach-25-Nov-22.pdf>

(artikel 3). Om ändamålet är annat än brottsbekämpning är risknivån hög (Annex III).

Vår analys är att tjänsten varken kvalar in på fjärridentifiering så som det definieras i artikel 5 eller Annex III. Detta för att båda utgår från att individen inte aktivt söker att bli identifierad. I myndigheternas föreslagna tjänst är individen själv aktiv part i att identifieringen ska ske. Tjänsten utgör alltså inte en förbjuden användning av AI eller en verksamhet som kräver certifiering enligt AI-förordningen.

Däremot är *Cyber Resilience Act* (CRA²⁴) värd att beakta. I CRA, Annex III, listas kritiska produkter med digitala element som utgör risk. Där återfinns (inte uttömmande):

- Identity management systems and privileged access management software (Class I 1)
- Password managers (Class I 3)
- Security information and event management, SIEM (Class I 10)
- Public key infrastructure and digital certificate issuers (Class II 3)

Dessa produkter ska certifieras och CE-märkas vilket kräver involvering av ett anmält organ (Annex VI, enligt modul C följt av modul B eller enligt modul H). Certifiering av produkter med digitala element lämnas utanför analysen och därmed avslutas diskussionen om identifiering. Däremot kan det finnas andra skäl att återkomma till certifiering av säkerhetskritiska element i relation till offentlig förvaltnings verksamhet och uppdrag.

Språkmodellen kvalar in under General Purpose AI (GPAI) så som det definieras i artikel 3, AI-förordningen: ett AI system som utför generella funktioner likt bild- och taligenkänning, video- och bild-generering, mönsterigenkänning, översättning etc. De kan användas i ett flertal olika kontexter. Kraven på GPAI specificeras i artikel 4a – 4c, vilket inkluderar CE-märkning.

CE-märkning av GPAI

GPAI ska uppfylla anpassningar av kraven i art 8–15 enligt implementerande akter som kommer tas fram av kommissionen efter att akten antagits (artikel 4b). Den som tillhandahåller systemet där språkmodellen ingår ska sätta ut sitt namn eller varumärke på systemet eller förpackningen (art 16aa), se till att systemet genomgår en försäkran om överensstämmelse för internkontroll

²⁴ European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, Brussels 15th September 2022: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0454&qid=1671521428931>

enligt Annex VI p 3+4 (artikel 16e), registrera systemet (artikel 51), vidta korrigerande åtgärder om systemet inte når de tekniska kraven beskrivna i artikel 8–15 (artikel 16g), CE-märka systemet och om behörig myndighet begär det visa överensstämmelse med artikel 8–15.

Artikel 48 hänvisar till Annex V som specificerar vad som ingår i en försäkran om överensstämmelse. Teknisk dokumentation ska finnas under 10 år från det att systemet erbjuds på marknaden. Den som tillhandahåller GPAI ska ge information till andra som vill använda systemet som ett högrisksystem, för att dessa ska kunna uppfylla kraven i AI-förordningen.

Annex VI är den certifieringsprocess som tillämpas när man inte måste ha med ett anmält organ. Det är alltså samma process som gäller för AI-system som berörs enligt Annex III. Den består av fyra steg:

1. Själv-certifiering görs enligt steg 2–4
2. (Tillhandahållaren verifierar att kvalitetshanteringssystemet överensstämmer med kraven i artikel 17 – den här punkten faller bort, enligt artikel 4b.3 är bara punkt 3 och 4 tillämpliga för GPAI)
3. Tillhandahållaren verifierar att den tekniska dokumentationen överensstämmer med de tekniska kraven (artikel 8–15)
4. Tillhandahållaren verifierar att det system som satt på plats för marknadsuppföljning är konsistent med kraven i artikel 61 och den tekniska dokumentationen

När ett AI-system genomgår en omfattande uppdatering (*substantial modification*) ska det anses som att AI-systemet har avslutat sin livscykel och att en ny version av systemet placerats på marknaden (artikel 3.1a). Det följer då rimligen att systemet ska certifieras på nytt om det anses ligga inom högriskdefinitionen eller är ett GPAI. Ett system som genomgår omfattande uppdateringar på grund av en planerad förmåga att utvecklas efter att det placerats på marknaden ska inte anses vara ett nytt system (artikel 3.23). Lärandet ska då preciseras i den medföljande dokumentationen och fortsatt spegla systemet. Tillämpningen av begreppet omfattande uppdatering ska preciseras av kommissionen genom en riktlinje efter att förordningen antagits (artikel 58a).

Konceptet omfattande uppdatering är relevant eftersom många av myndigheternas AI-tjänster kommer vara så kallade mikro-tjänster, eller en domänspecifik adaptering av en generell tjänst för ett specifikt ändamål. Den här sortens inkrementell förändring av ett AI-system som både medför att systemet är under konstant utveckling men också finns i flera versioner kommer kräva en genomtänkt strategi för att säkerställa att dokumentationen

stämmer överens med varje specifik version av tjänsten utan att det blir för resurskrävande.

Tekniska krav enligt AI-förordningen

Ibland hänvisar man i AI-förordningen till de tekniska kraven som kapitel 2, titel 1 och ibland som artikel 8–15. Vi kommer för enkelhetens skull använda begreppet de tekniska kraven. Följande är en kort genomgång av kraven som de står i akten. Hur de kommer se ut när akten är antagen är fortfarande en förhandlingsfråga samtidigt som kommissionen kommer initiera standardisering i relation till artiklarna (artikel 40 och 41) och ge mer detaljerade regler på hur kraven ska se ut för GPAI (artikel 4b).

Det finns ett utkast från kommissionen till standardiseringsorganen CEN och CENELEC om begäran av standarder²⁵ Följande är alltså en övergripande presentation som det finns anledning att återkomma till.

Artikel 8 är en inledande bestämmelse om att hög-risk AI ska uppfylla de tekniska kraven i kapitlet utifrån rådande *state of the art*. Här hade man önskat att det i artikeln även framgick att kraven gäller för GPAI, nu måste man läsa artiklarna 4a-4c för att veta det.

Artikel 9 slår fast att det ska finnas ett risk-hanteringssystem. Det är ett vanligt krav inom CE-märkning av produkter. Här kan det vara värt att komma ihåg att risk- och mitigationsanalys för mjukvara inte nödvändigtvis är detsamma som för mekatroniska system, det vill säga, de strategier som lämpar sig för säkra hissdörrar eller sågklingor är inte nödvändigtvis de som fungerar bäst för integritetsskydd eller automatiserade beslutsstöd vid myndighetsutövning.

Artikel 10 berör data-kvalitet och hantering. Data för träning, validering och testning ska vara relevant och representativ samt i görligaste mån komplett och felfri. Det ska bedömas i relation till ändamål och användare vilket är en svårare uppgift att avgränsa för GPAI än specialbyggda system med en tydligare uppgift. Kommissionens klagörande kommer bli viktigt för att veta hur man ska värdera ett representativt översättningssystem inom svensk myndighetsutövning.

Artikel 11 beskriver kraven på teknisk dokumentation. Artikeln hänvisar till Annex IV där mer finns att se om vad som ska ingå i dokumentationen. En sak

²⁵ European Commission, Draft standardisation request to the European Standardisation Organisations in support of safe and trustworthy artificial intelligence, Brussels 5th December 2022: <https://artificialintelligenceact.eu/wp-content/uploads/2022/12/AIA---COM---Draft-Standardisation-Request-5-December-2022.pdf>

som nämns är relationen till relevanta harmoniserade standarder. Uppfyller man dem uppfyller man också motsvarande tekniska krav. Att veta vilka standarder som finns och vilka som är på gång är alltså en viktig pusselbit för att vara i överensstämmelse med kraven. En dialog med SIS och andra standardiseringsorganisationer kan underlätta.

Artikel 12 berör vikten av loggar och vad som ska loggas.

Artikel 13 Artikel 13 beskriver vikten av att kunna förstå hur systemet fungerar och att det ska vara tydligt vad systemet kan förväntas lära sig självt efter att det satts på marknaden, med mera. Därför ska det framgå vad som kan vara ett förväntat resultat, vad indata bör vara, vilken hårdvara som krävs för att systemet ska fungera som förväntat osv.

Artikel 14 berör relationen till användaren av systemet. Det är inte alltid lätt att veta vem som är användare – om en medborgare fyller i uppgifter för att få ut en förmån eller ett bidrag, är det hen som är användare då? Eller är det myndigheten? Det är en viktig fråga att besvara eftersom användarens skyldigheter bland annat omfattar att kunna göra en konsekvensanalys utifrån artikel 35 i GDPR (artikel 29). Det ska vara möjligt för en användare att realisera sitt ansvar genom lämpliga interventionsmöjligheter samt veta systemets begränsningar så det används för rätt ändamål. Utbildning och löpande information kommer bli viktiga delar av systemutvecklingen och behöva kopplas till myndigheternas interna riktlinjer för AI-användande. Det blir också viktigt att tydliggöra när systemet är ansvarigt och inte.

Artikel 15 lyfter till sist kraven på cyber-säkerhet. Om man uppfyller kraven som ställs i *Cyber Resilience Act* så uppfyller man också kraven i artikel 15. Det framgår om man läser den senare akten men inte utifrån artikel 15. I relation till cyber-säkerhet bli det viktigt att dels se hur de tekniska kraven anpassas för GPAI, dels se systemgränserna för översättningssystemet. Ett exempel på det är huruvida översättningen visas på en skärm (jämför Google translate) eller automatiskt blir indata till ett beslutsstödsystem.

Rekommendationer

Vi ser en vikt av att myndigheterna fortsätter arbeta med hur svensk förvaltning ska dels ha kompetens och förmåga att använda sig av AI-system när det främjar genomförandet av myndigheternas uppdrag, dels utvecklar den förmågan för att kunna hantera de regulatoriska krav som kommer från EU i relation till AI som teknologi och cyber-säkerheten som dessa system behöver garantera.

Arbetet kan ta flera riktningar beroende på vad som anses mest relevant och utifrån vilka resurser som ges. En förståelse av de kommande standardernas relation till de tekniska kraven i artikel 8–15 blir betydande. Dessa standarder ska utifrån EU:s grundläggande rättigheter säkerställa datakvalitet, rätt form av loggning och mänsklig översyn med mera.

I relation till hur förvaltningsgemensamma system utvecklas och används blir det också viktigt att förstå hur domänspecifika anpassningar ska kunna göras i överensstämmelse med den tekniska dokumentationen samt användarens möjligheter att leva upp till de krav på ansvar som ställs. Här finns också frågor om hur myndigheterna kan fortsätta att använda sig av öppen mjukvara i sin egen utveckling då fler krav ställs på certifiering av ingående komponenter.

Användningen av personuppgifter för att träna AI-system är också aktuell. Dels för att många av myndigheternas system kommer hantera personuppgifter, dels för att AI-förordningen möjliggör träning av AI-system på existerande personuppgifter inom regulatoriska sandlådor även om uppgifterna samlats in för andra syften än systemutveckling. Vi ser därför också att erfarenheter av att anordna och bedriva verksamhet i form av regulatoriska sandlådor är betydelsefullt för svensk förvaltning. De erfarenheterna kommer ge välbehövligen kompetenser för myndigheternas nya roll som innovationspartner²⁶ samt ge en grund inför förhandlingar på EU-nivå om hur och varför regulatoriska sandlådor ska upprättas.

Arbetet kan med fördel bedrivas inom ett eller flera policylabb där deltagarna har möjlighet att utforska nya regulatoriska krav i relation till pågående systemutveckling.

RISE Research Institutes of Sweden AB

Håkan Burden
hakan.burden@ri.se
 +4673 052 02 29

Susanne Stenberg
susanne.stenberg@ri.se
 +4673 398 73 41

²⁶ H. Burden and S. Stenberg, Regulating Trust – An Ongoing Analysis of the AI Act, Gothenburg 5th December 2022:
<http://urn.kb.se/resolve?urn=urn:nbn:se:ri:diva-61344>