

Förstudie - Etablera förutsättningar för AI

2024-10-17

Skribenter: Ann-Louise Ekestubbe, Björn Bergqvist, Fredrik Hallgren,
Henrik Alfredsson och Patrik Sällström

Projektledare: Eva Lidslot

Versionshantering

Datum	Version	Beskrivning	Ändrat av

Innehåll

1 Inledning	2
1.1 Bakgrund	2
1.2 Om förstudien.....	2
1.3 Avgränsningar	2
1.4 Förutsättningar	3
1.5 Identifierade resurser för AI-tjänster	4
1.6 Rekommendation	6
2 Om AI	8
2.1 Produkter och tillämpningar inom AI	8
2.1 Effektivisering och automatisering utifrån Als förmågor	10
2.2 Infrastruktur för AI	11
2.3 Risker med AI	14
3 Nödvändiga förmågor och tjänster inom Göteborgs Stad	16
3.1 Kompetenscenter för Digitalisering	16
3.2 Intraservice	17
3.3 Nödvändiga förmågor hos stadens förvaltningar och bolag	18
3.4 Tekniska förmågor: MLOps och Data Management	19
4 Tekniska roller kopplade till AI	23
4.1 Data Scientist	23
4.2 AI-specialist	23
4.3 Dataingenjör	23
4.4 DevOps-specialist	23
4.5 Integritets- och säkerhetsexpert	24
4.6 IT-arkitekt	24

1 Inledning

1.1 Bakgrund

Digitalisering i Göteborgs Stad definieras som verksamhetsutveckling med stöd av digitala teknologier, inklusive AI-teknologier som påverkar stadens aktiviteter i stor utsträckning. AI kan förstås som en samling sociotekniska teknologier som påverkar människor, organisationer, samhället och teknologisk utveckling.

Samhället står idag vid en teknologisk skiljeväg där artificiell intelligens (AI) snabbt omformar ekonomiska och sociala landskap globalt. Denna framväxt drivs av betydande teknologiska framsteg inom djupinlärning och neurala nätverk, vilket möjliggör revolutionerande tillämpningar inom områden som hälso- och sjukvård, utbildning och säkerhet. Tillgången på data och framsteg inom hårdvaruteknik, såsom grafikprocessorer, har accelererat utvecklingen och implementeringen av AI-system.

Utvecklingen stöds också av omfattande investeringar från både privat och offentlig sektor, vilket understryker behovet av politisk vägledning och reglering för att säkerställa att innovationerna bidrar positivt till samhället, med respekt för etik och integritet. Göteborgs Stad har en avgörande roll i att forma framtiden för AI, för att främja innovation samtidigt som medborgarnas rättigheter och välfärd skyddas.

1.2 Om förstudien

Användningen och tillämpningen av artificiell intelligens ses som en tydlig trend och en självklar utveckling. Intraservice behöver därför utreda och föreslå vilka centrala leveranser som behöver anpassas för att möta förväntad utveckling inom området samt vilka centrala leveranser som är möjliga och lämpliga att erbjuda staden för att stödja dess digitalisering kopplat till AI. I Göteborgs Stads budget för 2024 pekas AI ut som ett område där Intraservice har ett särskilt ansvar. Syftet med förstudien är att reda ut centrala begrepp på området samt identifiera nödvändiga förmågor och leveranser inom staden, med särskilt fokus på Intraservices roll kopplat till förändringen mot en ändamålsenlig IT- och verksamhetsarkitektur i Göteborgs Stad.

1.3 Avgränsningar

Förstudien fokuserar på möjliggörare för tillämpning av AI i form av kompetens och digital infrastruktur. Leverantörer på marknaden arbetar redan med eller erbjuder olika typer av AI-baserad funktionalitet där varje produkt och tjänst behöver bedömas individuellt. Exempel på detta är Microsoft Co-Pilot och AI Swedens projekt "Digital assistent för offentlig sektor". Användningen av sådana produkter och tjänster ställer krav på tillgängliga resurser för exempelvis granskningar med fokus på

IT-säkerhet, arkitektur och datahantering. Sådant nyttjande innebär ofta en ökad kostnad för konsumtion av hårdvara, mjukvara eller licenser, vilket behöver beaktas inför varje enskild implementering.

1.4 Förutsättningar

Utvecklingen kopplat till artificiell intelligens sker i mycket hög takt, vilket gör det svårt att förutse vad som kommer att ske inom området på längre sikt. För att öka möjligheterna för Göteborgs Stad att ta del av de möjligheter som AI skapar krävs en stabil organisation med specifika kompetenser och förmågor samt möjligheter till snabb anpassning av planerade och pågående insatser inom området.

I samtal med bland annat Gartner och vid omvärldsbevakning ses en tydlig trend mot att börja resan med en "molnet-först"-strategi, där mindre affärskritiska tillämpningar som hanterar mindre känslig data testas för att på så sätt lära och stegvis växla upp mot mer affärskritiska lösningar där mer känslig data kan hanteras på ett kontrollerat sätt. Att börja med molnet först minskar även risken för överinvestering i kapacitet inom datacenterleveransen.

Då Göteborgs Stad i många delar fortfarande bygger upp förmågor kring datadelning, dataanalys och tillämpning av AI- och BI-verktyg är det viktigt att genomföra en kontrollerad resa och säkerställa att AI tillämpas på ett korrekt och kontrollerat sätt för att minimera risken för "övertillämpning". I grunden är tillämpning av AI till stor del en fråga om data. Genom att skapa förutsättningar för korrekt, stabil och säker hantering av data skapas förutsättningar för tillämpningar av såväl AI som BI.

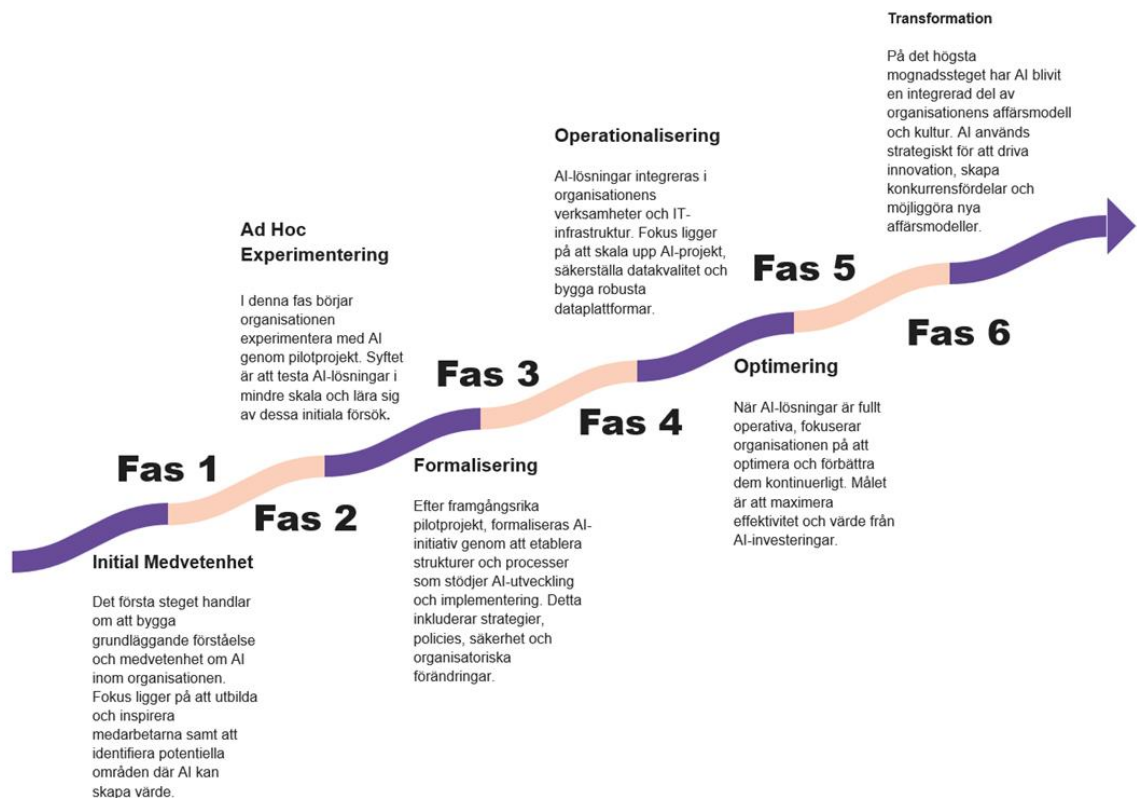
Då området är brett och komplext samt förknippat med initiativ på alla nivåer i samhället är det även viktigt att Göteborgs Stad har förmåga att tolka och hantera frågor rörande juridik, etik, riktlinjer, policys och strategier för området. I nuläget är AI Act och NIS2 aktuella, men området kommer sannolikt se ytterligare regelverk, ramverk och krav på styrning över tid.

I arbetet är det även viktigt ur ett Intraserviceperspektiv att leverera en plattform för resterande delar av staden att nyttja för att utveckla och tillämpa AI tillsammans med övriga marknaden.

I nuläget pratar man generellt om specifika tillämpningar där verksamheterna själva eller tillsammans med leverantör utvecklar specifika applikationer. I omvärldsanalysen ses en tydlig trend mot att fler och fler produkter rör sig mot olika typer av AI-funktionalitet, vilket sannolikt kommer ställa förändrade krav på underliggande infrastrukturleveranser framöver. Ett sådant nyttjande innebär ofta en ökad kostnad för konsumtion av hårdvara, mjukvara eller licenser, vilket behöver beaktas inför varje enskild implementering.

1.5 Identifierade resurser för AI-tjänster

För att möjliggöra en koordinerad och kontrollerad utvecklingsresa kopplat till AI bör mognadstrappan i bilden nedan följas där utvecklingen sker etappvis.



Figur 1: Mognadstrappa för AI-utveckling

Göteborgs Stad bedöms idag befinna sig runt fas 1–2, med lokala avvikelser. Nedan kostnadsangivelser är preliminära och kan komma att förändras då stadens behov och utvecklingen på området är svåra att förutse. För att fortsätta resan bör följande steg genomföras:

Fas 3 – Etablera arbetssätt och processer

Fas 3 innebär att etablera processer och arbetssätt som stödjer utvecklingen av AI. I detta ingår att sprida kunskap, identifiera relevanta användarfall och öka stadens förståelse och förmåga generellt kring AI. En framgångsfaktor för lyckad implementering av AI är etablering av ett kompetenscenter för AI. Exempel på arbetsområden för ett sådant center är samordning, kunskapsdelning, kompetensutveckling, styrning och policyutveckling, övervakning och extern samverkan. För att stödja detta ses roller motsvarande dataspecialist och AI-specialist som nödvändiga. I denna fas kan vissa mindre användarfall och piloter utföras baserat på befintliga tjänsteerbjudanden, men för större skala och utväxling i staden krävs fas 4 eller högre.

För att genomföra denna fas uppskattas kostnaden till 3 miljoner kronor per år. Kostnadsfördelningen behöver beaktas, och rekommendationen är att fördela kostnaden som en separat gemensam tjänst för att undvika ökad overhead.

Fas 4 – Operationalisering

Fas 4 innebär att AI-lösningar integreras djupare i stadens verksamheter och IT-infrastruktur. Fokus ligger på att skala upp relevanta AI-projekt, säkerställa datakvalitet och tillhandahålla robusta plattformar. För att nå denna fas behöver Intraservice sätta upp ett dedikerat team som ansvarar för att stödja staden i etablering och leverans av digital infrastruktur.

Leveranserna baseras på Intraservices befintliga tjänster och erbjudanden, där en eller flera kan nyttjas tillsammans för att möta stadens behov. Teamet behöver även ansvara för strategier, policys och säkerhetsaspekter relaterade till leveransen. Här krävs att teamet har kompetenser inom bland annat Azure, OpenShift, IT-säkerhet, övervakning samt identitet och åtkomst. För att stödja staden i denna fas behöver Intraservice även erbjuda en central hantering av data genom ett datalakehouse. I denna fas krävs tvärfunktionellt samarbete och att Intraservice möter staden på ett högre plan där rådgivning och uppsättning av infrastrukturen sker samlat. Här aktualiseras behov av koordinering och stöd i avrop av tjänsteerbjudanden från digital infrastruktur.

Uppskattad kostnad för denna fas är 6 miljoner kronor per år. Kostnaden avser förstärkning och etablering av team för samordnad leverans av infrastruktur.

Etablering av tjänst och tjänsteerbjudanden för leverans av datalakehouse är pågående och sker separat och inkluderas inte i denna uppskattning.

Fas 5 – Optimering

I fas 5 flyttas fokus till att optimera befintliga AI-lösningar för att maximera nyttan för verksamheterna. För att kunna stödja staden i denna fas krävs en ytterligare formalisering av de erbjudna AI-relaterade tjänsterna. Detta innebär att tillsätta en förvaltningsledare samt rekrytera en IT-arkitekt och en integritets- och säkerhetsexpert med särskild kompetens inom AI-relaterade frågor. Intraservice kan då erbjuda en mer sammanhållen tjänsteleverans kopplat till AI och möta staden på en högre nivå gällande deras AI-relaterade behov.

Fas 6 – Transformation

För att nå fas 6 krävs att staden har avancerat långt i sin AI-resa, etablerat egen kompetens inom datahantering och är redo att driva förändring inom den egna verksamheten. Här sätter stadens behov ramarna, men för Intraservice handlar det om att bygga vidare på det som etablerats i tidigare faser för att ge staden de verktyg som krävs.

1.6 Rekommendation

Etablera förmåga för att nå fas 3 och 4 under 2025 och 2026

Genom att förstärka Kompetenscenter för Digitalisering med utförande resurser inom AI och genom att etablera förmågor att hantera leveranser av nödvändig digital infrastruktur ses det som nödvändigt att skapa utrymme för att påbörja en förflyttning inom Intraservice mot fas 3 och 4 under 2025 och 2026. Kostnaden för en sådan förflyttning motsvarar 9 miljoner kronor per år, med en lägre kostnad 2025 med hänsyn till tidsåtgång för rekrytering. Kostnaden är en preliminär uppskattning och kan komma att behöva justeras utifrån stadens behov och önskad leveransnivå inom området.

Det är även viktigt att beakta att tillämpningen av AI kommer att kräva utökade volymer i Intraservices befintliga leveranser, såsom molnplattform, beroende på vad som konsumeras av respektive kund. Uppkommer ökade krav kopplat till drift av mer resurskrävande applikationer som ska driftsättas internt kan även detta generera en initial kostnad kopplat till inköp av hårdvara såsom grafikkort. Denna kostnad är inte medräknad ovan.

Molnet först

Vid samtal med Gartner har en "molnet-först"-strategi lyfts fram för att undvika stora investeringar i infrastruktur innan behovsbilden är helt fastställd. De grafikkort som ofta nyttjas för AI är dyra i inköp och innebär ofta en relativt hög energiförbrukning. För att undvika investeringar innan behovsbilden är klarlagd rekommenderas att i den mån det är möjligt börja arbetet med AI i de molntjänster som finns på marknaden för att vid behov gå över till en egen lösning (on-premises). Det är viktigt att beakta att molntjänster är förknippade med ett antal andra viktiga frågor som behöver beaktas särskilt, såsom behandling av information och personuppgifter, obehörig åtkomst och andra säkerhetsrisker.

Kubernetesbaserade lösningar i egen drift

Vi kommer att utforska och lära oss vad som krävs för att implementera Kubernetesbaserade lösningar i egen drift för AI-applikationer. Genom att undersöka och förstå våra behov kan vi bättre avgöra hur en lokal Kubernetesplattform kan möta kraven på högre klassad informationssäkerhet och stödja våra mål.

Prioritera arbetet med datalakehouse

Korrekt hantering av stora mängder data är i många fall en förutsättning för tillämpning av AI. För att stärka Göteborgs Stad i arbetet med att få

en ökad kontroll över sin data och för att möjliggöra ett mer datadrivet arbetssätt är det pågående projektet "Etablera tjänst för datalakehouse" en grundläggande förutsättning. Det är även viktigt att hela staden ökar sin förmåga kring data management för att möjliggöra ett mer datadrivet arbetssätt.

Se över funktioner för compliance, dataskydd, juridik och övervakning för området (governance)

I samband med användning av AI kommer behovet av stöd kring dataskydd, övervakning, juridik och etik att öka. Exempel på relevanta frågor som behöver hanteras är påverkan från AI Act, NIS2, GDPR, användning av molntjänster, klassificering av information och lösningar. Utveckling av policys och riktlinjer sker på kommunal, regional, statlig och internationell nivå, och därför är omvärldsbevakning och tolkning viktiga perspektiv att beakta.

Börja i mindre skala

För att möjliggöra innovation och starta upp arbetet med AI ses det som lämpligt att börja i mindre skala och med lösningar som inte är verksamhetskritiska, samt avvakta med att skapa lösningar som hanterar särskilt känslig information, påverkar beslutsprocesser eller myndighetsutövning eller på andra sätt kan påverka den enskilde.

Utveckling ska ske i enlighet med ramverk för IT- och verksamhetsarkitektur

I en snabbt föränderlig marknad kommer det snart att finnas ett brett utbud av produkter och tjänster där AI tillämpas för olika behov. För att undvika personberoenden och minska den tid som krävs för utveckling, förvaltning och support av skräddarsydda applikationer i egen regi, rekommenderas att använda beprövade komponenter och lösningar inom infrastrukturen. Exempelvis finns det för Kubernetes etablerade riktlinjer för komponentanvändning, och i Azure finns "Well-Architected Framework" som beskriver bästa praxis för byggande. Vid behov kan vi också överväga att köpa färdiga lösningar, särskilt om vi vill komplettera en befintlig applikation med specifika AI-funktioner.

2 Om AI

2.1 Produkter och tillämpningar inom AI

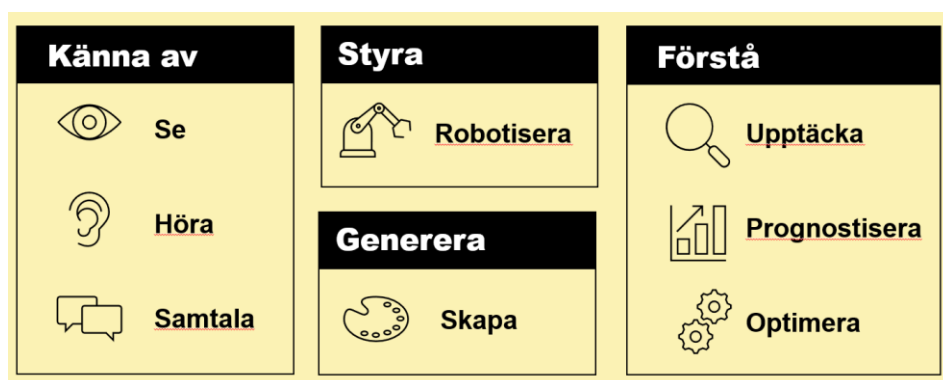
Produkter och tillämpningar byggda på AI i stadens verksamhet syftar på olika kanaler, teknologier och system som utnyttjar artificiell intelligens för att förbättra tjänster, effektivisera processer och stödja beslutsfattande inom kommunen. Det är i dessa kanaler och tillämpningar som den verkliga nyttan uppstår, så stor vikt måste läggas på slutanvändare och att lösningen är ändamålsenlig. Rätt utformade kan dessa AI-baserade lösningar hjälpa till att hantera en mängd olika uppgifter och utmaningar som Göteborgs Stad står inför, vilket resulterar i bättre service för medborgarna och mer effektiv intern förvaltning.

Exempel på tillämpningar inkluderar:

- **Digitala assistenter för medarbetare** som automatiserar hantering av vanliga frågor och frigör tid för personalen.
- **Intelligenta trafikstyrningssystem** som analyserar realtidsdata för att optimera trafikflöden, vilket minskar trängsel och utsläpp.
- **Förebyggande underhåll** för olika typer av infrastruktur.
- **Optimering av scheman, rutter eller lokaler** genom ett mer behovsbaserat arbetssätt.
- **Övervakning av energi- och vattenförbrukning** för att upptäcka fel och avvikelser.
- **Analys av folkhälsodata** för att förebygga sjukdomar.
- **Individanpassat stöd inom utbildning** genom individuell analys, vilket förbättrar elevers skolprestationer.
- **Ökad offentlig säkerhet** genom att analysera data för att förebygga brott.

Genom att implementera AI-baserade produkter och tillämpningar kan Göteborgs Stad stärka sina leveranser, öka effektiviteten och ge bättre service till sina invånare.

Många av de tillämpningar vi nämner ovan bygger på en eller flera av de förmågor som AI kan ha, vilket visas i förenklad form i bilden nedan och beskrivs ytterligare i följande kapitel.



Figur 2: Förenklad bild av AI-förmågor

Många förvaltningar och bolag har liknande utmaningar där ett antal grundmodeller för AI och datahantering inklusive kvalitetskontroll kan återanvändas. Det krävs förståelse för vilka förmågor eller kombinationer av förmågor som behövs för att lösa de enskilda utmaningarna, och det är få AI-experter som behärskar alla; oftast är man expert inom ett område.

Tar vi exemplet om trafikstyrningssystem så är det en lösning som kombinerar bildanalys från övervakningskameror och tidsserieanalys från trafikflöden för att användas för att skapa en optimerad styrning (se, upptäcka, optimera och styra).

Maskininlärning

Maskininlärning (ML) är en gren inom artificiell intelligens där datorer lär sig från data för att förbättra sin prestanda på specifika uppgifter utan att explicit programmeras för varje enskild uppgift. Istället för att människor skriver instruktioner för att lösa ett problem, använder maskininlärning algoritmer som gör att datorer kan hitta mönster och samband i stora mängder data, och sedan använda dessa mönster för att fatta beslut eller göra förutsägelser. Maskininlärning kan användas för till exempel analys och uppskattningar av framtida flöden av trafik, vatten eller energi baserat på data från historiska flöden i kombination med till exempel väderdata.

Generativ AI

Generativ AI är en typ av artificiell intelligens som använder maskininlärningsalgoritmer för att skapa nytt innehåll baserat på data som den tränats på. Till skillnad från traditionella AI-system, som huvudsakligen fokuserar på att analysera och förstå data, har generativ AI förmågan att producera ny data, såsom text, bilder, musik eller annan typ av information.

Träningsprocessen för generativ AI är avgörande för modellernas prestanda och kräver stora mängder data för att lära sig mönster och skapa nya, liknande data. Denna process kan vara både tidskrävande och resursintensiv men är nödvändig för att generera högkvalitativa och realistiska resultat.

Generativ AI har en bred uppsättning tillämpningar. Inom bild- och videogenerering kan den skapa kommunikationsmaterial, förbättra bildkvalitet eller skapa hela videor. Inom textgenerering kan den skriva artiklar, riktlinjer, beslutsunderlag, projektdirektiv, poesi, kod och även simulera mänsklig interaktion genom chattbotar. Inom musik och ljud kan generativ AI skapa nya musikstycken, ljudlandskap eller efterlikna mänskliga röster. Inom spelutveckling används teknologin för att skapa nya spelmiljöer, karaktärer och berättelser dynamiskt.

Trots dess många fördelar väcker användningen av generativ AI också viktiga etiska frågor. Dessa inkluderar risken för att skapa falsk information eller intrång i upphovsrätten samt frågor kring transparens och ansvar. Det är därför viktigt att noggrant överväga de etiska implikationerna och implementera riktlinjer för att hantera dessa utmaningar på ett ansvarsfullt sätt.

2.1 Effektivisering och automatisering utifrån AIs förmågor

Vi ser två prioriterade områden som snabbt skulle kunna göra stor nytta i staden och som vi ser är möjliga att genomföra inom 1–2 år. Dessa områden är grundade på insikter från månatliga dialogmöten med skolförvaltningarna och socialförvaltningarna om deras behov relaterade till AI.

2.1.2 Digitala assistenter baserade på generativ AI för enklare informationshantering

En av de mest efterfrågade tillämpningarna är digitala assistenter som kan underlätta i det dagliga arbetet. AI-assistenter kan exempelvis ge enklare tillgång till information genom att snabbt och effektivt ge svar på frågor om aktuella styrdokument och riktlinjer som personal, såsom rektorer, lärare eller hemtjänstpersonal, behöver förhålla sig till i sina uppgifter. Dessa AI-assistenter kan även användas för att hjälpa medborgare och personal via plattformar som goteborg.se, goteborg.com, IT-support, kundsupport och EU-projektet CU som kommer skapa en AI-avatar i den digitala tvillingen.

För att driva utvecklingen av digitala assistenter har vi lanserat ett initiativ kallat AI-Speed, en innovationsprocess som pågår under sex månader. Inom ramen för AI-Speed stöttar vi 10–15 team från olika områden, såsom skolor, vård och omsorg, kundsupport, [Göteborg.se](https://goteborg.se), styrande dokument och det digitala navet. Målet är att utforska och möta de behov som dessa aktörer har uttryckt kring digitala assistenter, särskilt med fokus på de stora informationsmängder som är relevanta både för medarbetare och medborgare i staden.

I innovationsresan erbjuder vi stöd i flera steg. Först hjälper vi teamen att förstå sina utmaningar och behov samt att identifiera vilka användningsområden som är mest relevanta. Därefter kopplar vi in experter inom områden som IT-säkerhet, arkitektur, DSO och juridik för att säkerställa att lösningarna är robusta och hållbara. Vi genomför även nyttoanalyser och bygger prototyper, vilket gör det möjligt att utvärdera lösningarna praktiskt.

Efter innovationsprocessen tar vi fram två potentiella vägar framåt: antingen förberedelse för utveckling av tjänster inom Intraservice, eller skapande av bra upphandlingsunderlag för externa leverantörer. Genom att erfarenhetsdela och samarbeta med våra experter skapar vi en

gemensam lärandeprocess och driver flera spår parallellt för att maximera effekten och nyttan av de digitala assistenterna.

2.1.3 Förbättring av scheman och planering baserat på optimering

Ett annat viktigt område där AI kan göra stor skillnad är optimering av scheman och resursplanering. Inom både skola och vård kan AI användas för att automatisera och optimera scheman, ruttplanering, lokalplanering och fordonsunderhåll. Detta innebär att AI-algoritmer kan säkerställa att resurser används så effektivt som möjligt, samtidigt som tids- och kostnadsbesparingar görs.

Genom att implementera dessa AI-lösningar kan både förvaltningar och företag snabbt dra nytta av ökad effektivitet, minskad manuell arbetsbörda och bättre resursanvändning. Vi planerar att genomföra nästa AI-Speed inom detta område.

2.2 Infrastruktur för AI

För att möjliggöra effektiva AI-lösningar för Göteborgs Stad föreslås en hybridlösning av driftsplattformar där en kombination av molntjänster och egen drift utnyttjas. Denna strategi erbjuder flexibilitet, kostnadseffektivitet, säkerhet, låg latens, hög tillgänglighet och optimerad resursanvändning.

Genom att använda molntjänster kan till exempel utveckling och testning av AI-applikationer effektiviseras. Molntjänster erbjuder fördelar med dynamisk skalbarhet och kapacitetsanpassning efter faktiskt behov, vilket eliminerar problem med planering av prestanda och kapacitetsplanering som kan uppstå i lokal infrastruktur. Samtidigt finns det lösningar som av olika anledningar inte är lämpliga att hantera i molnet och därmed kräver drift i egen regi.

Denna kombination av molntjänster och lokal infrastruktur gör det möjligt att dra nytta av det bästa av två världar: snabb och flexibel utveckling i molnet samt stabil och optimerad drift på egen infrastruktur där det krävs. Detta tillvägagångssätt säkerställer att den ökade komplexiteten och de högre kraven som AI-applikationer ställer kan hanteras, samtidigt som en hög nivå av säkerhet och prestanda upprätthålls.

2.2.1 Kubernetesplattform i egen drift

Valet att använda en Kubernetesplattform för AI-applikationer drivs av flera centrala faktorer:

- **Säkerhet och dataskydd:** Hantering av känslig information kräver strikta säkerhetsåtgärder och ofta lokal lagring för att uppfylla lagkrav.

- **Kontroll över IT-infrastruktur:** En lokal lösning ger full kontroll, vilket kan förbättra tillgänglighet och prestanda genom att eliminera beroendet av externa nätverksförbindelser.
- **Ekonomiska aspekter:** Lokala lösningar innebär ofta större initiala investeringar men kan ge bättre kostnadskontroll och förutsägbarhet på lång sikt.
- **Integration med befintliga system:** Underlättar anpassning efter specifika behov.
- **Organisatoriska faktorer:** Lokal självbestämmanderätt och intern kompetens kan göra lösningar i egen drift mer attraktiva.
- **Riskhantering:** Minskat beroende av externa tjänster och kontroll över säkerhetskopiering och återställning.

Dessa faktorer är avgörande när beslut om en lokal lösning är rätt för våra behov.

2.2.2 Molnplattformar – IaaS/PaaS/SaaS

Flera faktorer påverkar valet av molnlösningar:

- **Kostnadseffektivitet:** Molntjänster erbjuds ofta via prenumerationsbaserade modeller där kunden betalar för det som faktiskt nyttjas, vilket minskar behovet av initiala investeringar.
- **Skalbarhet:** Möjliggör anpassning av resurser efter behov, vilket är särskilt användbart för lösningar med varierande krav.
- **Teknologisk tillgänglighet:** Molnlösningar erbjuder ofta den senaste teknologin utan behov av stora uppgraderingsprojekt.
- **Säkerhet:** De flesta molnleverantörer erbjuder avancerad säkerhetsinfrastruktur och inbyggd funktionalitet för efterlevnad av olika regelverk.
- **Effektivitet:** Automatiserade processer för säkerhetskopiering och kontinuitet frigör resurser för mer strategiskt arbete.
- **Flexibilitet:** Möjlighet att kombinera med olika tilläggstjänster för AI och dataanalys.

Det är viktigt att säkerställa att den data som är tänkt att hanteras lämpar sig för hantering i en molntjänst, särskilt med avseende på säkerhet och integritet.

2.2.3 Datalakehouse

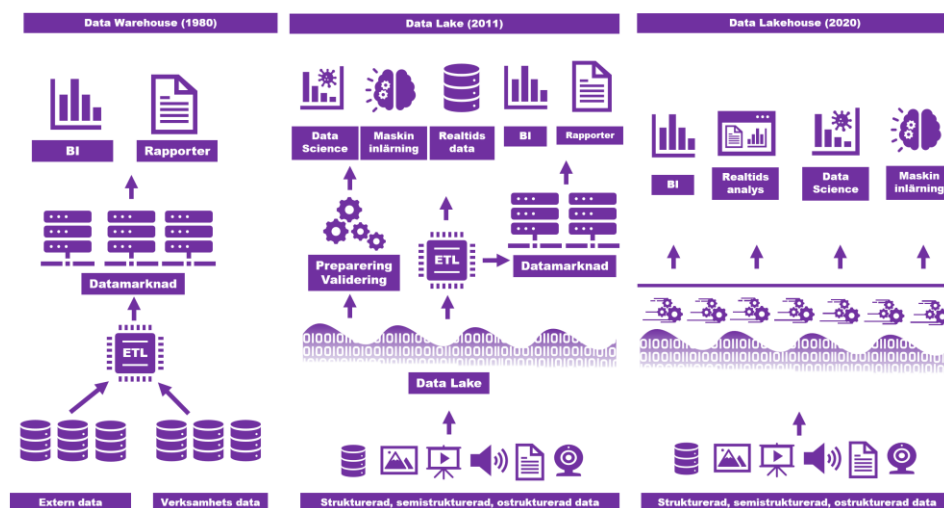
Ett datalakehouse kombinerar det som tidigare varit känt som datalake och data warehouse i en gemensam arkitektur där olika typer av data kan lagras och hanteras i en enhetlig plattform. Detta innebär fördelar i form av ökad kostnadseffektivisering, skalbarhet och prestanda.

I praktiken används datalakehouse-arkitekturen för att samla in data från en mängd olika källor, bearbeta och omvandla dessa data, och lagra dem på ett sätt som möjliggör enkel och snabb åtkomst för analys. Genom likartad hantering och hantering av metadata kan användare på ett

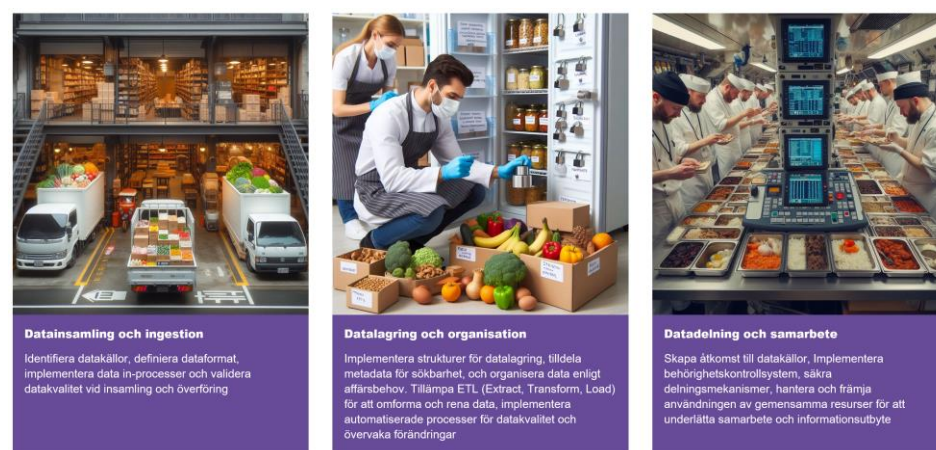
enklare sätt hitta data för vidare analys och hantering. Användare kan till exempel köra SQL-frågor, använda BI-verktyg eller köra AI-modeller direkt på lagrade data utan att behöva flytta den mellan olika system.

I Göteborgs Stads riktlinje för arkitekturprinciper nämns även tillgängliggörande av information särskilt i princip 6. Principen handlar om att säkerställa att data endast ska lämnas in en gång och därefter vara tillgänglig för dem som har rätt och behov att nyttja den. Principen belyser särskilt vikten av utpekade källsystem samt kontroll över datans ursprung.

Under 2024–2026 pågår ett projekt inom digital infrastruktur vars syfte är att etablera en tjänst för datalakehouse som kan avropas av stadens verksamheter. Projektet kommer att arbeta med olika användarfall och utveckla tjänsten utifrån identifierade behov.



Figur 3: Utveckling av datalager



Figur 4: Förmågor inom datalakehouse

2.3 Risker med AI

Nedan anges ett urval av risker som är typiska kopplat till användning av olika AI-baserade system och tillämpningar.

Bristande transparens

I tillämpningar av AI kan det vara svårt att genomsöka hur resultatet har skapats och vilka underlag som resultatet bygger på. Detta, i kombination med resultat som ofta kan uppfattas ha en hög grad av säkerhet, kan bidra till att beslut fattas på felaktiga grunder. Det är därför viktigt att alltid utbilda medarbetare i att kritiskt granska genererat material och att ha tillräckliga kontrollfunktioner för testning, validering och övervakning på plats. Detta gäller särskilt om AI tillämpas i processer nära beslutsfattande och myndighetsutövning där särskilda krav ställs på transparens och insyn.

Bristande förståelse för AI, dess tillämpningsområden och dess begränsningar

Om AI används för att ersätta mänsklig kompetens och erfarenhet istället för att fungera som ett kompletterande och stödjande verktyg kan potentiellt allvarliga konsekvenser uppstå, såsom driftstopp i kritisk infrastruktur eller åsidosättande av grundläggande demokratiska principer. Det är därför viktigt att medarbetare och chefer känner till respektive tillämpnings begränsningar och att mänskliga kvaliteter förstärks snarare än ersätts.

Otillräcklig datakvalitet

Om AI tillämpas på felaktiga eller ofullständiga data kan det generera resultat av bristfällig kvalitet, till exempel i form av konkreta felaktigheter eller som innehåller mått av diskriminering eller förutfattade meningar. En viktig del för att bemöta dessa risker är funktioner för testning, validering och övervakning, men även en ökad mognadsgrad gällande hantering av data.

Överdelning av data

Genom att tillämpa AI på data utan tillräckliga kontrollfunktioner kan information spridas till obehöriga användare genom överdelning av data. Detta kan uppstå på flera sätt, till exempel genom att data inte är korrekt anonymiserad, genom att AI-modellen får tillgång till mer data än vad som är relevant för tillämpningen, eller genom att AI-modeller integrerats i system där användare oavsiktligt ger modellen tillgång till data genom olika behörigheter eller annan behandling av data.

Överdriven tilltro till AI

Antalet tillämpningsområden för AI ökar i mycket hög takt, men det är viktigt att Göteborgs Stad och dess verksamheter är försiktiga i sina tillämpningar och säkerställer att AI faktiskt är rätt verktyg och att nyttan med respektive satsning säkerställs för att undvika "överhantering" av data och tillämpningar som är onödiga.

3 Nödvändiga förmågor och tjänster inom Göteborgs Stad

3.1 Kompetenscenter för Digitalisering

För att effektivt möta behovet från förvaltningar och bolag behöver man erbjuda en central förmåga som driver på arbetet och stöttar i transformationsresan som AI innebär. Vi rekommenderar att Kompetenscenter för Digitalisering förstärks ytterligare inom AI med resurser för utförande. Detta är ett strategiskt viktigt beslut för att maximera nyttan med AI-teknik på ett effektivt och ansvarsfullt sätt.

Anledningar till att ett sådant centrum är nödvändigt:

- **Samordning och kunskapsdelning:** Enligt nulägesanalysen pågår redan flera AI-initiativ inom olika delar av staden, men det saknas en sammanhållen styrning och koordinering mellan olika förvaltningar och bolag. Kompetenscenter för Digitalisering kan fungera som en central nod för att samordna dessa initiativ, vilket säkerställer att alla delar av staden arbetar mot gemensamma mål och delar med sig av erfarenheter och kunskap.
- **Kompetensutveckling och stöd:** Staden står inför stora utmaningar när det gäller kompetensutveckling inom AI. Kompetenscentret kan ta en ledande roll i att utforma och genomföra utbildningsprogram, stödja pedagoger och på så sätt höja stadens övergripande kompetensnivå inom AI.
- **Innovation och implementering:** Göteborg har initierat flera projekt där AI spelar en central roll för att förbättra både medborgarservice och interna processer. Kompetenscentret kan driva dessa innovationsarbeten vidare genom att erbjuda expertis och resurser för att utveckla nya AI-lösningar och skala upp framgångsrika pilotprojekt till bredare användning.
- **Styrning och policyutveckling:** Med tanke på den snabba teknikutvecklingen och de potentiella riskerna behövs starka ramar och tydliga riktlinjer. Kompetenscentret kan ansvara för att utveckla och uppdatera stadens riktlinjer för AI-användning, vilket garanterar att tekniken används på ett etiskt och juridiskt hållbart sätt.
- **Övervakning och utvärdering:** Kompetenscentret kan kontinuerligt övervaka och utvärdera hur AI används inom stadens olika verksamheter för att säkerställa att tekniken ger önskad nytta och för att identifiera områden som behöver justeras eller förbättras.
- **Extern samverkan:** Göteborg samarbetar aktivt med nationella och internationella partners. Kompetenscentret kan fördjupa dessa samarbeten och agera som stadens representant i dialoger med andra kommuner, akademiska institutioner och privata aktörer, vilket förbättrar tillgången till ny teknik och forskning.

Genom att förstärka Kompetenscenter för Digitalisering inom AI kan Göteborgs Stad systematiskt adressera de utmaningar och möjligheter som AI medför. Detta bidrar till teknisk och operativ excellens och stärker stadens förmåga att leverera högkvalitativa tjänster till medborgarna, samtidigt som man hanterar de etiska och juridiska frågeställningarna som tekniken medför.

3.2 Intraservice

3.2.1 Digital infrastruktur

Intraservice har inom digital infrastruktur redan idag flera tjänster, plattformar, tekniker och kompetenser på plats som kan nyttjas på olika sätt för att tillämpa AI. Exempel på sådana befintliga leveranser är kapacitet inom datacenter, containerteknik och molnplattformar, men även kommande tjänster såsom ett gemensamt datalakehouse som är under framtagning. Intraservice har därför en viktig roll i att möjliggöra för verksamheterna i staden att nyttja AI och dess möjligheter.

Det är viktigt att säkerställa att ansvarsfördelningen mellan Intraservice och respektive verksamhet blir tydlig. Digital infrastruktur på Intraservice bör i första hand leverera infrastruktur som möjliggör tillämpningar av AI, och det är verksamheten som ansvarar för dessa tillämpningar. Denna distinktion är viktig för att undvika att Intraservice blir en flaskhals och istället blir en stabil och säker plattform för resten av staden att bygga på. På detta sätt kan även marknaden nyttjas av staden genom inköp av exempelvis applikationer och konsulttjänster.

För att stödja staden och öka förutsättningarna för att nyttja AI behöver Intraservice, tillsammans med Kompetenscenter för Digitalisering, fokusera på att etablera förmåga att leverera relevant digital infrastruktur. För att möta staden ses därför ett behov av att påbörja etableringen av ett tvärfunktionellt team som involverar flera befintliga men även nya kompetenser. Bemanningen av teamet kommer behöva bestå av resurser med kompetens inom moln- och containerteknologi, identitet och åtkomst, informationssäkerhet, DevOps, MLOps, integration och automation samt data management.

Utöver teamet kommer utvecklingen inom AI ställa utökade krav på andra förmågor i form av exempelvis hantering och ägarskap av data och rollbaserad åtkomstkontroll.

3.2.2 Gemensamma tjänster

Förstudien har främst fokuserat på digital infrastruktur, men inom området för gemensamma tjänster ses ett ökat intresse från staden för såväl AI- som BI-lösningar. Exempel på behov inom området är AI kopplat till bemanning. Det finns även stor potential kopplat till tillämpningar inom ekonomi, HR och ledning och styrningsområdet. Här ses ett ökat behov av ytterligare samarbete med digital infrastruktur

framåt, och ett antal beroenden mellan såväl etablerade tjänster som planerade projekt har identifierats.

3.3 Nödvändiga förmågor hos stadens förvaltningar och bolag

För att effektivt möta verksamhetens behov av AI och med stöd av Kompetenscenter för Digitalisering ta hem nyttorna med AI, är det avgörande att förvaltningar och bolag utvecklar specifika roller och förmågor. Dessa kan delas in i fem huvudkategorier:

- **Ledarskap**
- **Förändringsledning**
- **Datasamordnare**
- **Tekniska förmågor**
- **Domänspecifik kunskap**

De tekniska förmågorna behöver initialt byggas upp av Intraservice, men för att skala upp användningen är det även rekommenderat att kompetensen på sikt även finns ute i verksamheterna.

Ledarskap

Ledningen inom varje förvaltning och bolag bör utse ett team som ansvarar för förvaltningens AI-arbete. Detta team har, i samarbete med Kompetenscenter för Digitalisering, det övergripande ansvaret för verksamhetens data- och analysstrategier.

Förändringsledning

Förändringsledare är centrala i att hantera den organisatoriska omställningen som AI-implementering innebär. Här är rollen som förändringsledare viktig, då de hjälper till att översätta tekniska lösningar till affärsnytta och säkerställer att medarbetarna förstår och accepterar förändringarna. Att ha förändringsledare med stark kommunikationsförmåga och engagemang är avgörande för att skapa en kultur som stödjer AI-utveckling. Regelbundna utbildningar och workshops kan hjälpa till att förbereda medarbetarna på de nya verktyg och teknologier som AI medför.

Informationsägarskap / Datasamordning

Det krävs ett förtydligande av informationsägarskap för att uppnå nyttan av AI. En förmåga som behöver stärkas är datasamordning inom verksamheternas domän med ansvar att säkerställa hög datakvalitet och effektiv datastyrning. De samlar in, kvalitetssäkrar och koordinerar datarelaterade aktiviteter inom sina områden. Detta är viktigt för att kunna leverera tillförlitliga data till AI-modeller och säkerställa att data används korrekt. Implementering av datahanteringsverktyg och metadatahantering underlättar detta arbete.

Tekniska förmågor

Inom tekniska förmågor är roller som dataingenjör, data scientist, AI-expert och IT-arkitekt centrala:

- **Dataingenjörer** ansvarar för att bygga och underhålla den datainfrastruktur som AI-applikationer kräver.
- **AI-expert och AI-utvecklare** arbetar med att utveckla och implementera AI-modeller.
- **Data scientists** analyserar data och utvecklar avancerade modeller för att lösa komplexa problem.
- **IT-arkitekter** designar de övergripande tekniska lösningarna som stödjer AI-initiativ.

Tillgång till en robust och säker teknisk infrastruktur, inklusive hybridmolnstrategier och GPU-kapacitet, är avgörande för att stödja dessa roller.

Domänspecifik kunskap

För att säkerställa att AI-initiativ är relevanta och effektiva är domänspecifik kunskap nödvändig. Roller som affärsanalytiker och domänexperter är viktiga för att identifiera och formulera problem som AI kan lösa inom specifika verksamhetsområden:

- **Affärsanalytiker** arbetar med att förstå verksamhetens behov och identifiera var AI kan skapa mest värde.
- **Domänexperter** använder sin djupa kunskap inom specifika områden för att bidra till utvecklingen av anpassade AI-lösningar.

Tvärfunktionella team som inkluderar dessa roller kan driva utvecklingen av AI-lösningar som är skräddarsydda för att möta unika behov inom olika delar av staden.

3.4 Tekniska förmågor: MLOps och Data Management

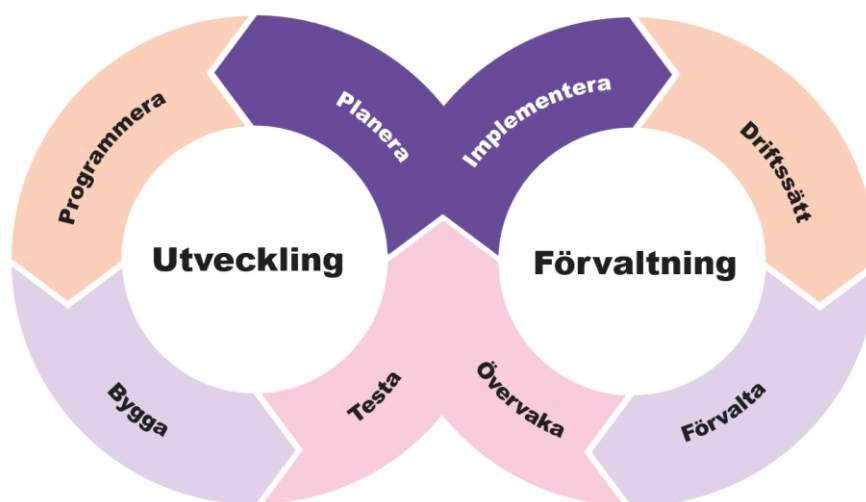
För att införa AI i en större verksamhet krävs en välorganiserad MLOps-enhet som inkluderar flera nyckelroller. **MLOps** (Machine Learning Operations) är en förmåga som kombinerar principer från maskininlärning och DevOps. Målet med MLOps är att säkerställa att maskininlärningsmodeller kan utvecklas, tränas, distribueras och övervakas på ett systematiskt och hållbart sätt, vilket blir särskilt viktigt med kraven från AI-förordningen.

Aktiviteter för MLOps:

- **Automatisering av livscykeln:** MLOps strävar efter att automatisera och effektivisera hela livscykeln för maskininlärningsmodeller. Detta inkluderar att skapa pipelines för kontinuerlig integration och distribution, vilket möjliggör

automatisk bygg, testning och distribution av modeller. Genom att använda dessa pipelines kan modeller snabbt och säkert sättas i produktion, vilket minskar tiden från utveckling till implementering.

- **Samarbete mellan team:** Ett annat viktigt syfte med MLOps är att främja bättre samarbete mellan olika team inom organisationen, såsom dataspecialister, AI-specialister, dataingenjörer och driftteam. Detta samarbete är avgörande för att säkerställa att alla aspekter av modellens livscykel hanteras korrekt, från datainsamling och förbehandling till modellutvärdering och övervakning.
- **Skalbarhet:** Skalbarhet är en central del av MLOps, då det säkerställer att maskininlärningslösningar kan hantera stora datamängder och komplexa modeller. Genom att designa system och processer som kan skala med ökande datavolymer och modellkomplexitet kan organisationen bibehålla prestanda och tillförlitlighet även vid stor användning.
- **Kvalitetssäkring:** Kvalitetssäkring är också en viktig del av MLOps. Genom att kontinuerligt integrera och testa modeller samt övervaka deras prestanda i produktion kan eventuella problem upptäckas och åtgärdas tidigt. Detta bidrar till att upprätthålla hög kvalitet och tillförlitlighet i maskininlärningsmodellerna.
- **Efterlevnad av lagar och regler:** MLOps säkerställer att alla modeller och databehandlingsprocesser följer relevanta lagar och regler, inklusive dataskydd och säkerhetsföreskrifter. Detta är särskilt viktigt inom offentlig sektor som kommuner, där dataskydd och integritet är kritiska.



Figur 5, översiktsbild över MLOPS

3.4.1 Data Management (Information Governance)

Vikten av att underlätta för datadelning, bearbetning och uppnå interoperabilitet

I takt med den snabba utvecklingen inom artificiell intelligens (AI) uppstår en unik möjlighet för Göteborgs Stad att stärka sin förmåga att arbeta mer strategiskt och systematiskt med data och den övergripande informationsstyrningen. För att nå en högre grad av datamognad och bli en mer datadriven organisation behöver staden genomföra en omfattande genomlysning av nuvarande datastyrning och hanteringsprocesser. Denna utveckling är inte bara nödvändig för att utnyttja potentialen i AI, utan också för att adressera flera kritiska områden som är avgörande för en hållbar och säker digital transformation.

AI och dess alltmer ökande betydelse skapar ett naturligt fokus på viktiga frågor som rör informationssäkerhet, arkitektur, datakvalitet och en djupare förståelse för hur verksamhetens data används och kan nyttjas effektivare. Dessa områden bildar tillsammans en stabil grund för att driva en framgångsrik digitalisering där AI fungerar som en motor som både accelererar och belyser behovet av att arbeta strukturerat med datakvalitet och genomtänkt livscykelhantering av data. Genom att använda AI som verktyg kan Göteborgs Stad förbättra insamling, analys och beslut baserade på data, vilket i sin tur bidrar till bättre tjänster för medborgarna och effektivare resursanvändning.

För att hantera stadens ökande dataflöden på ett effektivt och regelrätt sätt krävs en helhetslösning för att implementera och övervaka dataflöden end-to-end, från dataproducenter till datakonsumenter. Dessa dataflöden, eller "datapipelines", måste hanteras genom ett ekosystem av olika systemlösningar och plattformar, vilket innebär att utveckling och drift av dessa flöden måste vara både användarvänlig och säkerhetsmedveten. Målet måste vara att skapa bättre förutsättningar än idag för interoperabilitet vid bearbetning och datadelning.

Därför behöver Göteborgs Stad utveckla tjänster och verktyg som underlättar implementeringen av datapipelines över flera tekniska plattformar och organisatoriska gränser. Dessa tjänster ska främja en transparent och effektiv hantering av data och säkerställa att informationsflödet sker i enlighet med gällande lagar och regler. Genom att skapa strukturer för hur data samlas in, delas och analyseras kan staden säkerställa hög datakvalitet och att data nyttjas på ett sätt som genererar insikter och stöd för beslutsfattande.

Datakvalitet är avgörande för att AI-teknologier ska fungera effektivt och korrekt. Bristfälliga data kan leda till felaktiga slutsatser och ineffektiva beslut, medan högkvalitativa data möjliggör träffsäkra analyser och robusta AI-modeller. För att förbättra datakvaliteten behövs tydligt definierade processer för dataklassificering, aggregering och delning. Dessa processer måste också integrera regelverk och bästa praxis för

säker hantering av känsliga data, vilket kräver både teknisk kompetens och stark styrning inom informationssäkerhet.

Genom att fokusera på datakvalitet och livscykelhantering kan Göteborgs Stad säkerställa att rätt data används på rätt sätt, vilket i sin tur gör det möjligt för AI att skapa verkligt värde. Denna förbättrade datainfrastruktur skapar också möjligheter för staden att arbeta mer proaktivt med dataanalys och få djupare insikter i verksamhetskritiska frågor, såsom medborgarnas behov, trafikflöden, klimatåtgärder och resursfördelning.

För att Göteborgs Stad ska kunna dra nytta av AI och bli en mer datadriven organisation krävs en strategisk satsning på datastyrning, datakvalitet och informationssäkerhet. AI fungerar som en katalysator för denna utveckling genom att ställa krav på bättre datahantering och livscykelhantering. Genom att utveckla tjänster och verktyg som underlättar dataflöden och säkerställer hög datakvalitet kan staden optimera sin digitalisering och leverera mer värde till medborgarna. Denna resa mot en datadriven framtid kräver ett nära samspel mellan teknik, processer och människor, med fokus på att skapa långsiktigt hållbara lösningar i en genomtänkt IT- och verksamhetsarkitektur.

4 Tekniska roller kopplade till AI

För att framgångsrikt implementera och underhålla AI-lösningar inom Göteborgs Stad krävs ett antal specialiserade roller. Dessa roller är avgörande för att säkerställa att maskininlärningsmodeller utvecklas, implementeras och underhålls effektivt och säkert.

4.1 Data Scientist

En **data scientist** är ansvarig för att utveckla och träna maskininlärningsmodeller baserade på kommunens data och specifika behov. De utför utforskande dataanalys (EDA) för att identifiera mönster och insikter samt skapar relevanta funktioner (features) från rådata för att förbättra modellens prestanda. Dessutom designar och genomför de experiment för att utvärdera olika modeller och algoritmer samt bedömer modellernas prestanda med olika måttvärden för att säkerställa att de uppfyller de önskade kraven.

4.2 AI-specialist

En **AI-specialist** ansvarar för att implementera maskininlärningsmodeller i produktionsmiljöer och integrera dem med kommunens system. De säkerställer att modeller och system är skalbara och kan hantera stora datamängder. Deras uppgifter inkluderar att optimera modellernas prestanda, utveckla och underhålla pipelines för automatiserad datahantering, modellträning och distribution samt implementera övervakningsverktyg för att följa modellernas prestanda och upptäcka driftproblem i realtid.

4.3 Dataingenjör

En **dataingenjör** designar och hanterar processer för insamling av data från olika källor. De transformerar rådata till användbara format för maskininläring och säkerställer datakvaliteten genom att identifiera och åtgärda saknade eller inkorrekta data. De utvecklar och underhåller ETL-processer (Extract, Transform, Load) för att förbereda data för analys och modellträning samt designar dataarkitekturer som stödjer effektiv datalagring och åtkomst.

4.4 DevOps-specialist

DevOps-specialister skapar och underhåller kontinuerliga integrations- och distributionspipelines (CI/CD) för att automatisera bygg, testning och distribution av maskininlärningsmodeller. De hanterar infrastrukturen för att stödja maskininlärningsoperationer, inklusive servrar, databaser och molntjänster. De optimerar resurser och kostnader för infrastrukturen genom att använda skalbara och effektiva lösningar. Dessutom implementerar de system för övervakning och loggning av ML-

applikationer för att säkerställa tillgänglighet och prestanda samt ansvarar för incidenthantering och snabba lösningar av driftproblem.

4.5 Integritets- och säkerhetsexpert

En **integritets- och säkerhetsexpert** säkerställer att all data hanteras och lagras säkert med adekvata säkerhetsåtgärder för att skydda mot obehörig åtkomst och dataintrång. De implementerar och övervakar åtgärder för att skydda personuppgifter i enlighet med GDPR och andra relevanta lagar och regler. De bedömer och hanterar risker relaterade till dataintegritet och säkerhet i maskininlärningsprojekt samt säkerställer att alla aktiviteter följer lagstiftningen. Dessutom utvecklar och underhåller de incidentresponsplaner för att hantera säkerhetsincidenter och dataläckor snabbt och effektivt.

4.6 IT-arkitekt

En **IT-arkitekt** inom MLOps ansvarar för att designa och implementera den tekniska infrastrukturen som krävs för att stödja maskininlärningsoperationer. De utvärderar tekniska och operativa krav, kostnader samt säkerhetsaspekter för att välja den mest lämpliga driftplattformen, antingen on-premises eller i molntjänster som AWS, Azure eller Google Cloud. Målet är att hitta den plattform som bäst uppfyller projektens behov och stadens långsiktiga strategi.

IT-arkitekten samarbetar med olika team och intressenter för att säkerställa att de tekniska lösningarna stödjer verksamhetens mål. Detta innebär att arbeta nära data scientists och maskininlärningsingenjörer för att förstå deras behov och säkerställa att infrastrukturen stödjer deras arbete. De ger även teknisk rådgivning och stöd till projektledare och andra intressenter för att fatta välgrundade beslut om tekniska lösningar och strategier.