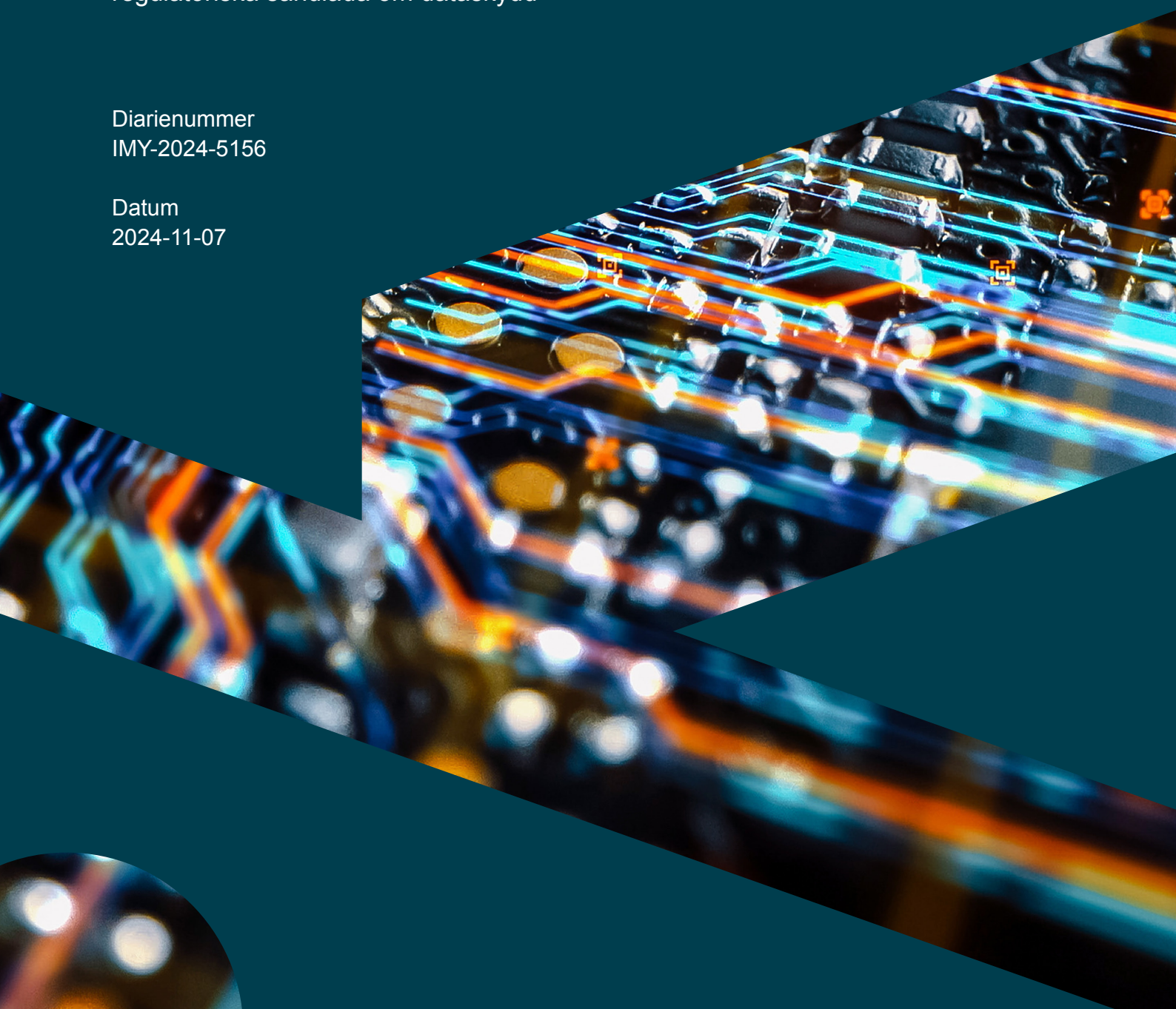
IMY. Integritetsskydds myndigheten

Utlämnande av allmänna handlingar med hjälp av AI

Slutrapport från Integritetsskyddsmyndighetens regulatoriska sandlåda om dataskydd

Diarienummer
IMY-2024-5156

Datum
2024-11-07



Integritetsskydds myndigheten

Diarienummer:
IMY-2024-5156

Datum:
2024-11-07

Utlämnande av allmänna handlingar med hjälp av AI

Innehållsförteckning

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

Sammanfattning

- **Integritetsskyddsmyndigheten (IMY) har under våren och sommaren 2024 genomfört sitt tredje projekt i myndighetens regulatoriska sandlåda.** Med regulatorisk sandlåda avser IMY fördjupad vägledning om hur dataskyddsregelverket bör tolkas och tillämpas. Kännetecknande för arbetssättet är att IMY tillsammans med den aktuella verksamheten identifierar de rättsliga frågor som vägledningen ska fokusera på. Vägledning ges därefter muntligt vid flera tillfällen under några månaders tid i form av workshops eller andra dialogbaserade former. Arbetet utmynnar i en publik rapport där resonemang och bedömningar sammanfattas för att möjliggöra ett lärande för fler.

- **Projektet ”Utlämnande av allmänna handlingar med hjälp av AI” är IMY:s tredje projekt.** Deltagarna i projektet har varit Lidingö stad och Atea Sverige AB (Atea). Målet har varit att undersöka några av de juridiska gråzonsfrågor som uppkommer när man önskar använda en AI-lösning som ett digitalt verktyg för att effektivisera delar av sekretessbedömningen inför utlämnandet av allmänna handlingar.

- **Projektet omfattar två huvudsakliga koncept:** ett mer omfattande system (helhetstjänsten) och ett mer avgränsat system (maskeringstjänsten). Helhetstjänsten avsågs automatisera stora delar av processen för utlämnande av allmänna handlingar, men under projektets gång visade det sig innehålla både tekniska och juridiska hinder. Deltagarna valde därför att fokusera på, och gå vidare med, maskeringstjänsten. Maskeringstjänsten syftar till att identifiera och ge förslag på uppgifter som ska maskeras i allmänna handlingar. Lösningen baseras på AI-drivna språkmodeller och ska kunna stödja handläggare i sekretessbedömningen. Maskeringstjänsten är alltså endast ett handläggarstöd vilket innebär det är en handläggare som i slutändan beslutar om vad som ska omfattas av sekretess och inte.

- **Användningen av maskeringstjänsten förväntas medföra betydande effektivitetsvinster** genom att automatisera den initiala identifieringen och maskeringen av personuppgifter i allmänna handlingar. Deltagarna har uppgett att dagens manuella sekretessmaskering är en tidskrävande och arbetsintensiv process för handläggare, särskilt när stora volymer handlingar har begärts ut. Genom att låta maskeringstjänsten göra en preliminär maskering, där både direkta och indirekta personuppgifter identifieras, kan handläggare frigöra tid och resurser som annars hade gått åt till manuellt arbete. Detta möjliggör en snabbare och mer effektiv hantering av utlämningsprocessen och stärker kommunens förmåga att uppfylla tryckfrihetsförordningens krav på skyndsamhet.

- **Vägledningen i projektet har fokuserat på tre rättsliga frågeställningar.** Utöver dessa frågeställningar finns också andra juridiska frågor som behöver beaktas innan en AI-tjänst kan driftsättas, men som inte har analyserats inom ramen för projektet.

- **Fråga 1: Finns det rättslig grund för användningen av en AI-tjänst vid utlämnande av allmänna handlingar?** IMY har analyserat om det kan finnas rättsligt stöd i dataskyddsförordningen och kompletterande svensk rätt för behandling av personuppgifter, inklusive känsliga personuppgifter, som sker i samband med användningen av AI-tjänsten för hantering av begäranden om allmänna handlingar. IMY har som utgångspunkt bedömt att det kan finnas rättslig grund för användningen av både helhetstjänsten och maskeringstjänsten i uppgifter av allmänt intresse. Samma grund kan också som utgångspunkt vara stöd för behandling av känsliga personuppgifter i båda tjänsterna. I fråga om krav på nödvändighet och proportionalitet i sammanhanget, anser IMY att mycket talar för att behandling av både ”vanliga” och känsliga personuppgifter i maskeringstjänsten kan ha rättslig grund. Däremot talar övervägande skäl emot att behandling av personuppgifter i helhetstjänsten är nödvändigt och proportionerligt i dagsläget, särskilt gällande känsliga personuppgifter.

- **Fråga 2: Hur fördelas personuppgiftsansvaret?** Enligt IMY är det mycket som talar för att personuppgiftsansvaret är avgränsat till den enskilda kommunen, medan AI-leverantören (Atea i detta projekt) agerar som personuppgiftsbiträde. Vidare finns det flera omständigheter som talar för att var och en av nämnderna är separat ansvarig för den personuppgiftsbehandling som sker när maskeringstjänsten används. Den enskilda nämnden bär således det slutgiltiga ansvaret för att säkerställa att de allmänna handlingar som begärs ut har sekretessmaskerats korrekt.

- **Fråga 3: Vad kan vara lämpliga säkerhetsåtgärder vid användningen av AI-tjänsten?** IMY bedömer att en konsekvensbedömning avseende dataskydd bör göras innan AI-tjänsten tas i bruk. Rekommenderade säkerhetsåtgärder innefattar särskild styrning och ökad riskmedvetenhet vid användning av AI inom organisationen, men innefattar även stark autentisering, kryptering, loggning samt regelbunden övervakning för att förhindra obehörig åtkomst och felaktig databehandling. Det krävs även en tydlig och transparent kontroll över vilka data AI-modellen har tillgång till samt att all hantering sker i överensstämmelse med dataskyddsförordningen. IMY understryker särskilt vikten av att säkerställa att ”human-in-the-loop” efterföljs, vilket bland annat innebär att ansvariga handläggare självständigt behöver säkerställa att sekretessmaskeringen är korrekt innan handlingen lämnas ut.

Integritetsskyddsmyndighetens regulatoriska sandlåda om dataskydd

Med regulatorisk sandlåda avser Integritetsskyddsmyndigheten (IMY) **fördjupad vägledning om hur dataskyddsregelverket bör tolkas och tillämpas**. Inget undantag ges från reglerna i dataskyddsförordningen eller dess kompletterande lagstiftning utan vägledningen baseras på gällande rätt.

Kännetecknande för arbetssättet är att:

- IMY och innovationsaktörerna tillsammans identifierar de rättsliga frågor som vägledningen ska fokusera på,
- vägledning ges muntligt vid flera tillfällen under några månaders tid i form av workshops eller andra dialogbaserade former, och
- resonemang och bedömningar från vägledningen sammanfattas och publiceras i en rapport för att möjliggöra lärande för många.

1. Inledning

Användning av artificiell intelligens (AI) ökar i takt med den tekniska utvecklingens framsteg och digitaliseringen av samhället. Kommuner och andra offentliga aktörer står inför en förändring där AI spelar, eller kommer att spela, en central roll för att effektivisera och öka kvaliteten av till exempel administrativa processer och ändamålsenliga tjänster till medborgarna. Digitaliseringspolitikens övergripande mål är att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter.[1] Målet för digitaliseringen av den offentliga förvaltningen är en enklare vardag för medborgare, en öppnare förvaltning som stöder innovation och delaktighet samt högre kvalitet och effektivitet i verksamheten.[2] Digitalt ska vara förstahandsval i den offentliga förvaltningens verksamhet och i kontakter med privatpersoner och företag, samtidigt som säkerheten och skyddet för den personliga integriteten ska säkerställas.[3]

Regeringen har bland annat tillsatt en AI-kommission med uppdraget att säkerställa att Sverige bättre ska tillvarata möjligheterna och hantera riskerna med AI. Uppdraget omfattar att föreslå åtgärder för en ökad AI-användning i offentlig förvaltning genom datadriven innovation och dataförsörjning.[4] Regeringen har också nyligen gett Myndigheten för digital förvaltning (Digg) och IMY i uppdrag att ta fram riktlinjer för användningen av generativ AI inom den offentliga förvaltningen i syfte att främja förvaltningens ändamålsenliga och effektiva användning av generativ AI.[5]

Digg har beräknat att Sverige skulle kunna göra stora vinster i form av bland annat högre produktivitet om AI-teknik skulle användas fullt ut i Sveriges offentliga förvaltning.[6]

Regeringen har alltså som mål att Sverige ska bli bättre på att nyttja AI för att förbättra välfärden och öka konkurrenskraften.[7] Användningen av AI-teknologier inom offentlig sektor ska främjas med målet att ge möjlighet att hantera framtida samhällsutmaningar och utveckla effektiva offentliga tjänster. För att nå upp till målet behöver offentliga aktörer stödja den fortsatta AI-tillämpningen på olika sätt. Det kan ske genom att exempelvis tillhandahålla data eller samverka kring en nationell digital infrastruktur. Det behövs även stöd och vägledning inom olika områden. IMY har här en viktig roll att spela genom att ge vägledning om dataskydd och integritet. Ett sätt för IMY att ge vägledning är genom myndighetens regulatoriska sandlåda om dataskydd. I sandlådan ges vägledning i gråzonsfrågor som berör många. Resultaten presenterats i en publik rapport så att alla kan ta del av vägledningen. Vägledningen är tänkt att ge stöd i tolkningen och tillämpningen av dataskyddsregelverket.

Användningen av stora språkmodeller (eng. *large language models, LLM*) har under de senaste åren på många sätt revolutionerat hur vi ser på AI. En stor språkmodell är i grunden ett system som genom sannolikhetsfördelningar av sekvenser av ord bland annat kan användas för att skapa nya texter baserade på mycket stora textmängder. En stor språkmodell är en typ av generativ AI.[8]

---

[1] Prop. 2011/12:1 utg. omr. 22, bet. 2011/12: TU1, rskr. 2011/12:87.
[2] Prop. 2024/25:1 utg. omr. 22.
[3] Prop. 2018/19:1 utg. omr. 2.
[4] Kommittédirektiv dir. 2023:164, Förstärkt AI-förmåga i Sverige, s. 1 och 4.
[5] Regeringsbeslut 2024-07-04, Fi2024/01535.
[6] Delrapport i regeringsuppdraget I2019/01416 samt I2019/01020.
[7] Regeringskansliet, Nationell inriktning för artificiell intelligens, 2018, N2018/03008, s. 5, 8 och 10.
[8] Internetkunskap, Språkmodell (https://internetkunskap.se/artiklar/ordlista/sprakmodell).

Generativ AI kan beroende på tillämpningsområde bland annat användas för att automatisera rutinmässiga uppgifter både i den offentliga och privata sektorn. Med hjälp av AI kan till exempel kommuner snabbare tillhandahålla efterfrågad information, vilket skulle öka transparensen och tillgängligheten av allmänna handlingar för medborgarna.[9]

Implementeringen och användningen av AI kräver ett noggrant förarbete där bland annat dataskyddsregelverket behöver beaktas. Dataskyddsregelverket och särskilt dataskyddsförordningen (GDPR)[10] ställer krav på hur personuppgifter får behandlas och under vilka förutsättningar personuppgifter exempelvis får lämnas ut. För kommuner innebär detta att användning av AI för hantering av allmänna handlingar behöver genomföras med omsorg för att säkerställa att integritetsskyddet upprätthålls. Vidare behöver kommuner ha rutiner för riskbedömning och dataskyddsanalys på plats för att identifiera och hantera potentiella risker kopplade till AI-användningen. IMY:s tredje rapport i myndighetens regulatoriska sandlåda – Utlämnande av allmänna handlingar i en kommun med hjälp av AI – kommer att beröra några av dessa delar.

[9] Se vidare avsnitt 2 nedan.
[10] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

2. Projektet ”Utlämnande av allmänna handlingar med hjälp av AI”

2.1. Projektets deltagare

Lidingö stad är en kommun i Stockholms län med cirka 49 000 invånare. Kommunen hade redan påbörjat sin AI-resa innan det här projektet startade och har idag flera andra AI-relaterade projekt i sin portfölj. Just det här projektet om utlämnade av allmänna handlingar har hos kommunen gått under arbetsnamnet ”Rätt till insyn”. Kommunen har tillsammans med Kungsbacka kommun, Skaraborgs kommunalförbund, Linköpings universitet och advokatfirman Kahn Pedersen beviljats finansiering av Verket för innovationssystem (Vinnova) för att driva projektet vidare där den här rapporten tar slut.[11]

Atea Sverige AB (Atea) är ett svenskt it-företag som bland annat specialiserar sig på att leverera it-lösningar till både offentlig och privat sektor. Bolaget hanterar, driftar och utvecklar dess kunders it-miljöer. Atea bistår Lidingö stad i projektet med bland annat teknisk expertis.

Observatörer under projektet

Research Institutes of Sweden (RISE) har under workshop-serien deltagit i form av observatörer. RISE utvärderar IMY:s arbetssätt med regulatoriska sandlådor om dataskydd i ljuset av AI-förordningens[12] bestämmelser om regulatoriska sandlådor för AI.[13] RISE:s roll har framför allt inneburit att lyssna in under projektets gång och skaffa sig en bild över hur arbetet med IMY:s regulatoriska sandlåda om dataskydd bedrivs i praktiken.

2.2. Projektets mål

Det ursprungliga projektet: Helhetstjänsten

Initialt presenterade deltagarna ett omfattande projekt med en AI-driven helhetslösning för utlämnande av allmänna handlingar. Tanken var att allmänheten skulle kunna efterfråga handlingar och uppgifter genom ett grafiskt chattgränssnitt på kommunens hemsida. Målsättningen var att utveckla en tjänst som, genom ett automatiserat tillvägagångssätt, skulle kunna hitta och ta fram de begärda handlingarna, göra en preliminär sekretessbedömning av dem och föreslå maskering av sekretessbelagda uppgifter. Därefter skulle en medarbetare hos kommunen granska underlaget innan handlingen lämnades ut. I denna rapport benämns denna tjänst som ”helhetstjänsten”.[14]

---

[11] Målet med projektet är att ta fram en prototyp av en AI-lösning genom att ”undersöka och dokumentera vad som krävs rättsligt för att en AI-modell ska kunna användas vid avidentifiering och utlämning av allmänna handlingar samt ta fram och utveckla den tänkta AI-modellen”. Mer information om projektet finns på Vinnovas webbplats (https://www.vinnova.se/p/ratt-till-insyn/).
[12] Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens).
[13] Se artiklarna 57–58 i AI-förordningen.
[14] Se vidare avsnitt 3.2 nedan om de tekniska specifikationerna.

Det reviderade projektet: Maskeringstjänsten

Under projektets gång valde deltagarna att avgränsa projektet då man såg både juridiska och tekniska hinder för helhetstjänsten. Istället valde man att fokusera på en mer avgränsad tjänst som stödjer medarbetarna i att identifiera direkta och indirekta personuppgifter samt göra en preliminär sekretessbedömning av allmänna handlingar. Detta ansågs innebära färre tekniska och juridiska hinder, samtidigt som det fortfarande bedömdes ge ett stort mervärde. Denna AI-tjänst ska kunna lämna förslag till medarbetaren om bland annat vilka personuppgifter som kan vara sekretessbelagda. Medarbetaren granskar sedan AI-tjänstens bedömning och ansvarar för att handlingen har sekretessmaskerats på ett korrekt sätt i enlighet med gällande sekretessbestämmelser innan handlingen slutligen lämnas ut. Detta har varit den huvudsakliga infallsvinkeln för projektet och det som Lidingö stad och Atea har valt att fokusera på. I denna rapport benämns denna tjänst som ”maskeringstjänsten”.

Behov och ändamål

I denna rapport avses med begreppet ”sekretessbedömning” att identifiera och markera uppgifter i en allmän handling vilka kan omfattas av sekretess, främst med stöd av bestämmelserna i offentlighets- och sekretesslagen (2009:400), OSL. Denna prövning sker i samband med att en begäran om att få ta del av en allmän handling enligt offentlighetsprincipen görs. Härmed avses alltså inte den formella prövningen av om sekretess föreligger (så kallad myndighetsprövning[15]) utan de faktiska åtgärderna att gå igenom de allmänna handlingarna och maskera sådana uppgifter som kan vara belagda med sekretess (så kallat faktiskt handlande).

Lidingö stad har uppgett att det är sekretessbedömningen som är den delen av utlämnandeprocessen som idag kräver störst arbetsinsats. En AI-tjänst specialiserad på att hitta sekretessbelagda personuppgifter skulle därför vara till stor nytta för kommunen. Många kommuner, regioner och statliga myndigheter lägger ned mycket tid på att hantera sekretessbedömningar inom ramen för utlämnande av allmänna handlingar, vilket innebär att det finns ett stort intresse av klargörande vägledning inom detta område.

Lidingö stad vill effektivisera utlämnandeprocessen av allmänna handlingar genom att 1) använda språkmodeller för att identifiera direkta och indirekta personuppgifter i handlingar och 2) ge förslag på vilka uppgifter som kan omfattas av sekretess enligt OSL eller annan lagstiftning. Detta skulle frigöra tid och minska arbetsbelastningen för handläggare inom alla verksamhetsområden. Lidingö stad vill också öka myndighetens tillgänglighet och transparens samt i högre grad kunna uppfylla det skyndsamhetskrav som tryckfrihetsförordningen (TF) ställer på offentlig verksamhet. Kommunens avsikt är att AI-tjänsten ska användas som ett handläggarstöd vilket innebär att det är en handläggare som i slutändan ansvarar för att den allmänna handling som begärs ut sekretessmaskeras på ett korrekt sätt.

[15] Se 2 kap. 17 § TF och 6 kap. 2–3 §§ OSL.

2.3. Rättsliga frågeställningar

Lidingö stad och Atea enades tillsammans med IMY om att fokusera på följande rättsliga frågeställningar i det aktuella projektet:

- Finns det rättslig grund för användningen av en AI-tjänst för utlämnandet av allmänna handlingar i en kommun om AI-tjänsten fungerar som
  a) helhetstjänsten, eller
  b) maskeringstjänsten?

- Hur fördelas personuppgiftsansvaret?

- Vad kan vara lämpliga säkerhetsåtgärder vid användningen av AI-tjänsten?

2.4. Avgränsningar i projektet och annan upplysning

Eftersom ingen data kommer att överföras utanför Sverige har frågor kring dataöverföring till tredjeland inte analyserats.[16] Utgångspunkten är att behandlingen ska ske hos Lidingö stad och den avtalade leverantören, Atea.

Deltagarna har uppgett att man endast har använt fabricerade uppgifter inom ramen för detta projekt för att utvärdera olika modellers prestanda. Inom ramen för projektet har varken Lidingö stad eller Atea tagit fram eller tränat någon egen AI-modell, utan de har istället valt att använda en färdigtränad modell från en extern leverantör. Det innebär att frågor kopplade till bland annat insamling av träningsdata för att utveckla en AI-modell inte kommer att behandlas i denna rapport.

Det bör noteras att den aktuella AI-tjänsten inte är driftsatt och ytterligare juridiska och tekniska aspekter kommer behöva behandlas av deltagarna innan en driftsättning sker. Det kan exempelvis vara frågor som rör automatiserat beslutsfattande, insamling av träningsdata, de grundläggande principerna samt de registrerades rättigheter. Rapporten kommer heller inte att beröra AI-förordningen som trädde i kraft den 1 augusti 2024.

Denna rapport innehåller en redogörelse för IMY:s uppfattning i rättsliga frågor där det saknas vägledande domstolspraxis eller vägledning från Europeiska dataskyddsstyrelsen[17] (EDPB). Bedömningarna görs mot bakgrund av nuvarande rättsläge och kan komma att ändras om det skulle komma ny lagstiftning, domstolspraxis eller vägledning från EDPB.

Dataskyddsregelverkets tillämplighet

Förhållandet mellan dataskyddsregleringen och offentlighetsprincipen regleras i 2 kap. 7 § första stycket dataskyddslagen.[18] Enligt den bestämmelsen ska inte EU:s dataskyddsförordning eller dataskyddslagen tillämpas i den utsträckning det skulle strida mot bland annat regleringen om offentlighetsprincipen i 2 kap. TF. Denna rapport avser dock inte den personuppgiftsbehandling som krävs för att genomföra själva utlämnandet av allmänna handlingar enligt offentlighetsprincipen. Rapporten

[16] Mer information om så kallade tredjelandsfrågor finns på IMY:s webbplats (https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/overforing-till-tredje-land/).
[17] Läs mer om EDPB på IMY:s webbplats (https://www.imy.se/verksamhet/dataskydd/dataskydd-pa-eu-niva/edbp/).
[18] Lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

avser i stället användningen av digitala stöd för hantering av begäranden om allmänna handlingar enligt offentlighetsprincipen. Enligt IMY är dataskyddsregelverket tillämpligt på den personuppgiftsbehandling som sker med hjälp av sådana digitala stöd. Det innebär att dataskyddsförordningens bestämmelser om bland annat rättslig grund, personuppgiftsansvar och lämpliga säkerhetsåtgärder behöver beaktas.

3. Tekniken i projektet

3.1. Språkmodeller

Det har skett stora framsteg inom AI när det gäller att förstå och bearbeta språk. Idag kan AI användas för att analysera och sammanfatta långa texter, översätta dokument och skapa nya texter, såsom berättelser och historier. Denna kapacitet finns i så kallade språkmodeller, som är speciellt utformade för att utföra språkrelaterade uppgifter. Språkmodellerna lämpar sig för olika ändamål, bland annat utifrån krav på prestanda, resursanvändning och informationssäkerhet.

Stora språkmodeller

För att en språkmodell som är avsedd för ett brett användningsområde ska uppnå hög prestanda krävs ofta miljarder inlärda parametrar, vilket uppnås genom att bearbeta enorma mängder träningsdata. Denna träningsdata består vanligtvis av text och information som finns tillgänglig på internet och i andra digitala samlingar, som till exempel The Nordic Pile.[19]

Det höga antalet inlärda parametrar gör dessa modeller mycket kraftfulla och mångsidiga när det gäller språkförståelse. De här typerna av språkmodeller kallas för stora språkmodeller och kan vidareutvecklas för specifika syften. För att kunna anpassa en stor språkmodell eller använda den i en tjänst, körs den oftast på servrar hos en molntjänsteleverantör eller i ett lokalt datacenter med tillräcklig prestanda.

Meta är ett av flera företag som utvecklar stora språkmodeller och har till exempel lanserat sin öppna källkodsmodell Llama 3. Andra företag som OpenAI och Google har också utvecklat stora språkmodeller, såsom GPT-4o och Gemini. AI Sweden, RISE m.fl. har tagit fram den stora språkmodellen GPT-SW3 som är särskilt anpassad för de nordiska språken.[20]

Små språkmodeller

För att kunna använda språkmodeller på lokala enheter, såsom en persondator eller en mobiltelefon, där beräkningskraften är begränsad kan språkmodeller som är framtagna för mer specifika uppgifter istället användas. Då kan data bearbetas direkt i enheten istället för att behöva överföras via nätet genom en molntjänst. Små språkmodeller (eng. *small language model, SLM*) har ett färre antal inlärda parametrar, men kan ändå ha en tillräckligt hög prestanda för en mer specifik och avgränsad uppgift. Detta resulterar dock i en sämre förmåga för komplexa resonemang av generella uppgifter. De små språkmodellerna är ofta mer än hälften så stora som de stora språkmodellerna.

Instruktioner och träning

För att en språkmodell ska kunna utföra uppgifter baserat på användarens instruktioner behöver den vara tillräckligt tränad och ha förmåga att tolka instruktionerna korrekt. När man instruerar en modell, det vill säga när man promptar,

[19] The Nordic Pile, som är framtagen av AI Sweden, är en större samling av texter på de nordiska språken och används för att träna en språkmodell till att bättre förstå dessa språk (https://insights.ai.se/the-nordic-pile).
[20] AI Sweden, GPT-SW3 (https://www.ai.se/sv/projekt/gpt-sw3).

sker ingen ytterligare träning av modellen. Istället använder modellen den kunskap och de mönster som den har lärt sig under den ursprungliga träningsprocessen.

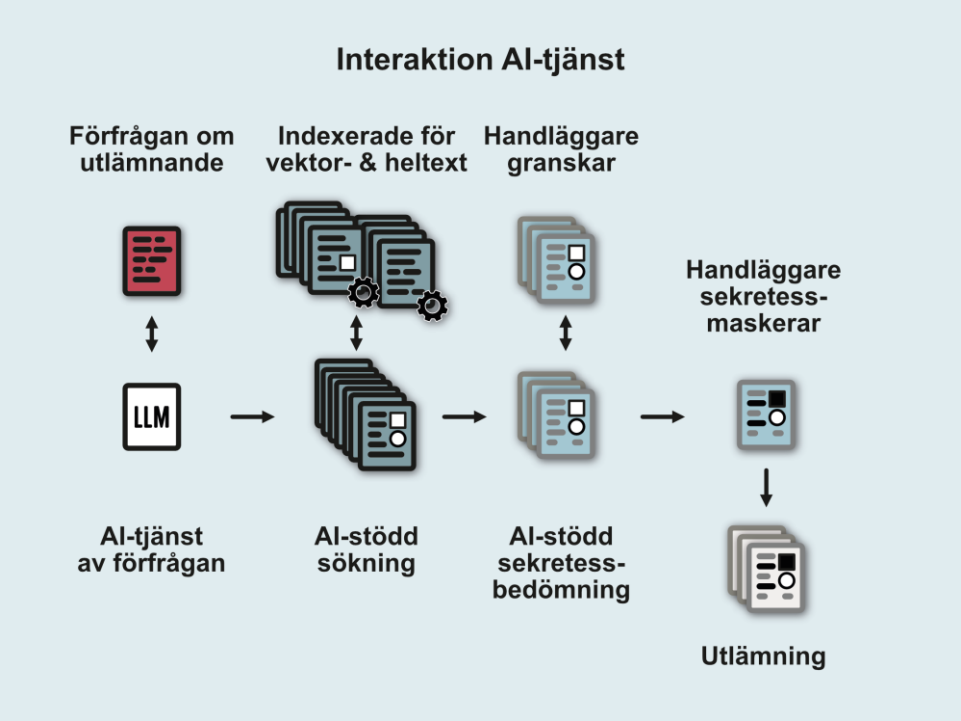
3.2. Tekniska specifikationer

Helhetstjänsten

Inom ramen för den ursprungliga idén med helhetstjänsten skulle en stor språkmodell ges tillgång till alla allmänna handlingar som kommunen förfogar över. Målet var att utveckla en chattbot som en användare skulle kunna interagera direkt med. Chattboten skulle kunna söka efter och hämta den information som användaren efterfrågade.

För att kunna realisera detta diskuterades användningen av stora språkmodeller i molntjänster. Dessa modeller saknar dock specifik kunskap om den information som finns hos Lidingö stad. För att skapa en chattbot som effektivt kan hämta och bearbeta kommunens data skulle därför en så kallad RAG-lösning (eng. *Retrieval Augmented Generation*) kunna implementeras. För att göra de allmänna handlingarna sökbara skulle de först behöva indexeras. Indexering är en metod för att organisera och strukturera data så att de kan sökas och hämtas effektivt.

I korthet var tanken att helhetstjänsten skulle fungera på följande sätt.



1. **Förfrågan** om ett utlämnande av allmänna handlingar inkommer.
2. Frågan **analyseras** av AI-tjänsten för att djupare förstå vad som efterfrågas.
3. En automatiserad **sökning** görs efter de handlingar som behövs för att besvara frågan (innebär att handlingar ur olika register indexerats för exempelvis **vektor- och heltextsökning**).

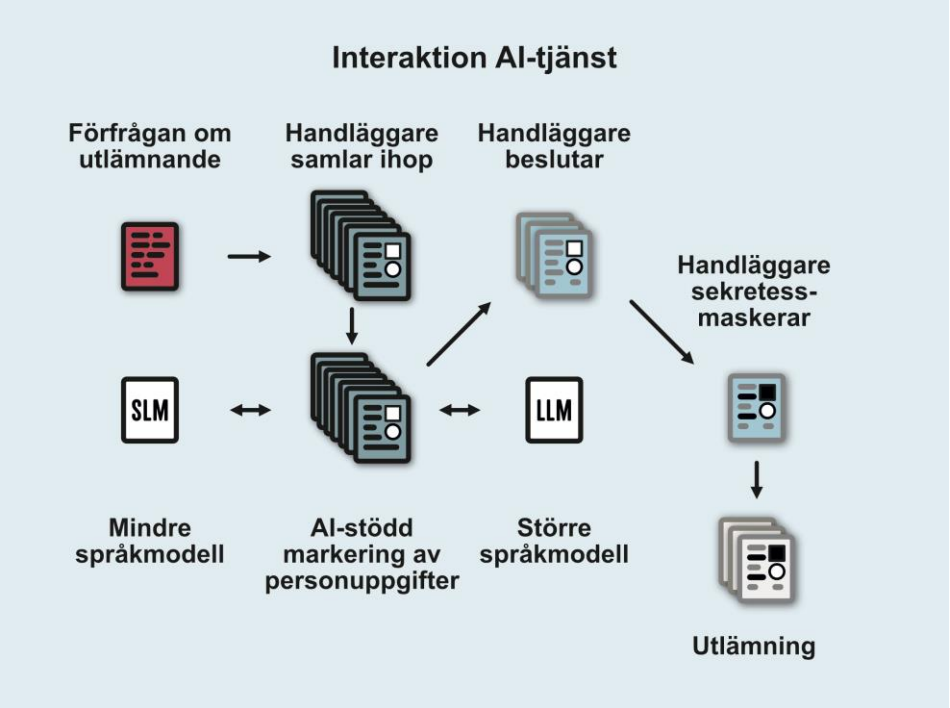
4. En **automatiserad sekretessbedömning** görs av samtligt föreslagna handlingar.
5. **Handläggare beslutar** om vilka uppgifter i handlingarna som ska **sekretessmaskeras**.
6. **Utlämnandet** sker via AI-tjänsten.

Maskeringstjänsten

Vad gäller maskeringstjänsten är tanken att använda både stora och små språkmodeller för textanalys. Först ska AI-tjänsten söka efter direkta personuppgifter i ett dokument, det vill säga i en allmän handling. Detta sker via i en mindre, lokalt placerad, språkmodell. Därefter görs en mer komplex sökning av direkta och indirekta personuppgifter, vilket sker med hjälp av en större språkmodell som körs på Ateas datacenter. AI-tjänstens färdigtränade språkmodeller behöver inte någon ny inlärning för att kunna utföra den tilltänka uppgiften. Modellen är statisk, vilket betyder att den inte kontinuerligt tränas eller uppdateras löpande med de data som modellen behandlar under användning.

Baserat på Ateas tester bedöms maskeringstjänsten kunna identifiera över 80 procent av personuppgifterna i en handling vilka ska sekretessmaskeras enligt lag vid en begäran om utlämnande.

I korthet är tanken att maskeringstjänsten ska fungera på följande sätt.



1. **Förfrågan** om ett utlämnande av allmänna handlingar inkommer.
2. Handläggare samlar ihop aktuella **allmänna handlingar**.
3. Handläggare använder maskeringstjänsten för **stöd i sekretessbedömningen** av handlingarna.

4. Maskeringstjänstens **mindre språkmodell analyserar** och markerar direkta personuppgifter i handlingarna.
5. Maskeringstjänstens **större språkmodell analyserar** och markerar direkta och indirekta personuppgifter i handlingarna.
6. **Handläggare beslutar** om vilka uppgifter i handlingarna som ska **sekretessmaskeras**.
7. **Utlämnandet** sker av handläggare.

4. Finns det rättslig grund för användningen av en AI-tjänst för utlämnande av allmänna handlingar i en kommun?

4.1. Dataskyddsförordningen

Av EU-domstolens praxis framgår att skyldigheten att på begäran lämna ut personuppgifter till allmänheten kan hänföras till den rättsliga grunden som kallas uppgift av allmänt intresse i artikel 6.1 e i dataskyddsförordningen.[21] Att allmänhetens rätt att få tillgång till allmänna handlingar kan betraktas som ett allmänt intresse anges också i skäl 154 till dataskyddsförordningen.

I samband med införandet av dataskyddslagen har regeringen bland annat uttalat följande.

> Enligt regeringens mening måste den grundlagsfästa rätten att ta del av allmänna handlingar anses utgöra ett viktigt allmänt intresse. Ordning och reda bland allmänna handlingar är enligt regeringen en förutsättning för att handlingsoffentligheten ska fungera och fylla sitt syfte. Den hantering av allmänna handlingar som krävs enligt svensk rätt är därför enligt regeringen motiverad med hänsyn till ett viktigt allmänt intresse. En stor del av denna hantering sker enligt regeringen i den elektroniska miljön och medför behandling av personuppgifter.[22]

Regeringens mer allmänna uttalanden i lagstiftningsärendet kan också nämnas.

> Alla uppgifter som riksdag eller regering gett i uppdrag åt statliga myndigheter att utföra är enligt regeringens mening av allmänt intresse. Om uppgifterna inte vore av allmänt intresse skulle myndigheterna inte ha ålagts att utföra dem. På motsvarande sätt är de obligatoriska uppgifter som ålagts kommuner och landsting att utföra av allmänt intresse. Begreppet uppgifter av allmänt intresse omfattar dock inte bara sådant som utförs som en följd av ett offentligrättsligt och uttryckligt åliggande eller uppdrag. Den verksamhet som en statlig eller kommunal myndighet bedriver, inom ramen för sin befogenhet, är således av allmänt intresse. Det är därmed den rättsliga grunden i artikel 6.1 e i dataskyddsförordningen som vanligen bör tillämpas av myndigheter, även utanför området för myndighetsutövning.[23]

Vad gäller bland annat den rättsliga grunden uppgift av allmänt intresse, ställer artikel 6.3 första stycket i dataskyddsförordningen krav på att grunden för behandlingen ska fastställas i EU-rätten eller i medlemsstaternas nationella rätt. Det är enligt regeringen ett utryck för legalitetsprincipen.[24] Enligt skäl 45 till dataskyddsförordningen krävs det inte en särskild lag för varje enskild behandling, utan det kan räcka med en lag som grund för flera behandlingar om behandlingen krävs för att utföra en uppgift av allmänt intresse. Enligt skäl 41 till dataskyddsförordningen krävs det heller inte nödvändigtvis en lagstiftningsakt antagen av ett parlament, men grunden bör vara tydlig och precis och dess tillämpning bör vara förutsägbar för personer som omfattas av den.

Av 2 kap. 2 § dataskyddslagen följer att personuppgifter får behandlas med stöd av artikel 6.1 e i dataskyddsförordningen om behandlingen är nödvändig för, såvitt här är

---

[21] Se EU-domstolens dom den 22 juni 2021, Latvijas Republikas Saeima, C-439/19, ECLI:EU:C:2021:504, särskilt punkt 120, även bl.a. punkterna 24, 34–37 och 99; samt EU-domstolens dom den 7 mars 2024, Endemol Shine Finland Oy, C-740/22, ECLI:EU:C:2024:216, bl.a. punkterna 46, 51 och 55.
[22] Prop. 2017/18:105 s. 86.
[23] Prop. 2017/18:105 s. 56 f.
[24] Prop. 2017/18:105 s. 49 ff.

relevant, att utföra en uppgift av allmänt intresse som följer av lag eller annan författning eller beslut som har meddelats med stöd av lag eller annan författning. Enligt regeringen är det inte själva behandlingen av personuppgifter som måste regleras, utan det är uppgiften av allmänt intresse som måste ha stöd i rättsordningen. I förarbetena anges vidare att det vid bedömningen av om något följer av exempelvis en lagbestämmelse kan bland annat förarbetsuttalanden, bestämmelsens syfte och den rättsliga kontext som bestämmelsen befinner sig i behöva beaktas.[25]

För att en behandling av personuppgifter med stöd av bland annat grunden uppgift av allmänt intresse ska vara tillåten måste behandlingen vara nödvändig för att utföra den aktuella uppgiften.[26] Enligt EU-domstolen innebär detta nödvändighetskriterium att det intresse som eftersträvas med behandlingen av personuppgifterna inte rimligen ska kunna uppnås på ett lika effektivt sätt genom andra medel som är mindre ingripande i de registrerades grundläggande fri- och rättigheter.[27] Regeringen har i samband med dataskyddsförordningens införande uttryckt saken som att behandlingen kan anses nödvändig om den leder till effektivitetsvinster.[28]

Vidare ställer artikel 6.3 andra stycket i dataskyddsförordningen krav på att syftet med behandlingen ska vara nödvändigt för att utföra en uppgift av allmänt intresse och att grunden ska vara proportionerlig. I bestämmelsen föreskrivs också att den fastställda grunden kan innehålla särskilda bestämmelser för att anpassa tillämpningen av dataskyddsförordningen.

EU-domstolen har i sin praxis ställt höga krav på utformningen av den rättsliga grunden.[29] Enligt regeringen måste det alltid göras en bedömning av personuppgiftsbehandlingens och verksamhetens karaktär för att avgöra hur stor grad av tydlighet och precision som krävs. Ett mer kännbart intrång kräver enligt regeringen en mer preciserad rättslig grund, medan en personuppgiftsbehandling med lägre integritetsrisker kan ske med stöd av en mer allmänt hållen rättslig grund.[30]

4.2. Nationell lagstiftning

För en kommun finns en mängd författningar som reglerar uppgifter av allmänt intresse, till exempel kommunallagen (2017:725) och olika materiella regelverk såsom socialtjänstlagen (2001:453). Bestämmelserna kompletteras ibland av sektorspecifika regleringar för personuppgiftsbehandling, så kallade registerförfattningar.

Rätten att ta del av allmänna handlingar, det vill säga offentlighetsprincipen, regleras av bestämmelserna i 2 kap. TF. Offentlighetsprincipen kan endast begränsas med hänsyn till de ändamål som anges 2 kap. 2 § TF, bland annat skyddet för enskildas

[25] Prop. 2017/18:105 s. 48 ff. och 188.
[26] Nödvändighetskriteriet följer av ordalydelsen i artikel 6.1 e i dataskyddsförordningen, se även skäl 39 till förordningen.
[27] Se t.ex. Latvijas Republikas Saeima, punkt 110.
[28] Prop. 2017/18:105 s. 189.
[29] EU-domstolens dom den 24 februari 2022, Valsts ieņēmumu dienests, C-175/20, EU:C:2022:124, punkt 83, där EU-domstolen uttalar följande: ”I detta sammanhang ska det dock erinras om att för att uppfylla det proportionalitetskrav som föreskrivs i artikel 5.1 c i förordning 2016/679 (se för ett liknande resonemang, dom av den 22 juni 2021, Latvijas Republikas Saeima (Prickning), C-439/19, EU:C:2021:504, punkt 98 och där angiven rättspraxis), måste de föreskrifter som ligger till grund för behandlingen innehålla tydliga och precisa bestämmelser som reglerar räckvidden och tillämpningen av den aktuella åtgärden samt ange minimikrav, så att de personer vars personuppgifter lämnas ut ges tillräckliga garantier för att uppgifterna på ett effektivt sätt är skyddade mot riskerna för missbruk. Dessa föreskrifter måste även vara rättsligt bindande enligt nationell rätt och i synnerhet ange under vilka omständigheter och på vilka villkor en åtgärd för behandling av sådana uppgifter får vidtas, vilket säkerställer att ingreppet begränsas till vad som är strikt nödvändigt (dom av den 6 oktober 2020, Privacy International, C-623/17, EU:C:2020:790, punkt 68 och där angiven rättspraxis)”.
[30] Prop. 2017/18:105 s. 51.

personliga eller ekonomiska förhållanden. Sådana begränsningar ska anges noga i en bestämmelse i en särskild lag eller, om det anses lämpligare, i en annan lag som den särskilda lagen hänvisar till. Bestämmelser om begränsningar av offentlighetsprincipen, det vill säga bestämmelser om sekretess, finns i huvudsak i OSL.

I OSL finns bestämmelser om att myndigheter ska beakta det intresse som enskilda kan ha av att själva utnyttja tekniska hjälpmedel för att söka efter och ta del av allmänna handlingar och att myndigheter i vissa fall på begäran ska tillhandhålla sådana hjälpmedel (4 kap. 1 § första stycket 4 och tredje stycket 1 samt 6 kap. 6 § första stycket OSL). Av förarbetena framgår bland annat att avsikten varit att bestämmelserna ska vara teknikneutrala och kunna uppnås i takt med den tekniska utvecklingen.[31]

OSL innehåller också en stor mängd bestämmelser om sekretess, bland annat till skydd för enskildas personliga förhållanden. Dessa sekretessbestämmelser förutsätter att det görs bedömningar av om bland annat personuppgifter kan lämnas ut till allmänheten. OSL reglerar dock inte vilka tekniska eller organisatoriska medel som kan användas för att underlätta sekretessbedömningar.

När det gäller skyldigheten att bedriva offentlig verksamhet på ett effektivt sätt kan bestämmelserna i 11 kap. kommunallagen om god ekonomisk förvaltning nämnas, liksom 3 § myndighetsförordningen (2007:515) och 9 § förvaltningslagen (2017:900). I förarbetena till dataskyddslagen anges att det bör anses vara nödvändigt att använda tekniska hjälpmedel, och därmed att behandla personuppgifter på automatisk väg, eftersom en manuell informationshantering inte utgör ett realistiskt alternativ för vare sig myndigheter eller företag. Vidare framgår det av förarbetena att det är ett viktigt allmänt intresse att myndigheternas ärendehandläggning kan ske på ett effektivt och rättssäkert sätt.[32]

4.3. Känsliga personuppgifter

Artikel 9 i dataskyddsförordningen innehåller bestämmelser som kompletterar bestämmelserna i artikel 6 i samma förordning gällande särskilda kategorier av personuppgifter. I Sverige kallas dessa uppgifter för känsliga personuppgifter.[33] Det framgår av artikel 9.1 vad som utgör känsliga personuppgifter och att behandling av sådana uppgifter som huvudregel är förbjuden.[34] I artikel 9.2 finns undantagen som beskriver när känsliga personuppgifter trots allt får behandlas.

Av artikel 9.2 g i dataskyddsförordningen framgår bland annat följande. Behandling av känsliga personuppgifter får ske om det är nödvändigt av hänsyn till ett viktigt allmänt intresse. Behandlingen ska ske med stöd av EU-rätten eller medlemsstaternas nationella rätt. Det innebär med andra ord att behandlingen kräver kompletterande rättsligt stöd för att vara laglig. Det kompletterande rättsliga stödet ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

---

[31] Jfr prop. 1981/82:37 s. 8 ff, s. 23–26 och 49–53 samt prop. 2008/09:150 s. 306–308 och 365.
[32] Prop. 2017/18:105 s. 47 och 87.
[33] Se 3 kap. 1 § dataskyddslagen om den svenska terminologin ”känsliga personuppgifter”.
[34] Känsliga personuppgifter är personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, samt genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa samt uppgifter om en fysisk persons sexualliv eller sexuella läggning.

Som nämnts ovan (se avsnitt 4.1) framgår av flera rättskällor att allmänhetens rätt att få tillgång till allmänna handlingar kan betraktas som ett allmänt intresse och ett viktigt sådant intresse.

En kompletterande nationell bestämmelse finns i 3 kap. 3 § dataskyddslagen. Där framgår bland annat följande.

> Känsliga personuppgifter får behandlas av en myndighet med stöd av artikel 9.2 g i EU:s dataskyddsförordning
> 1. om uppgifterna har lämnats till myndigheten och behandlingen krävs enligt lag,
> 2. om behandlingen är nödvändig för handläggningen av ett ärende, eller
> 3. i annat fall, om behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse och inte innebär ett otillbörligt intrång i den registrerades personliga integritet.
>
> Vid behandling som sker enbart med stöd av första stycket är det förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter.

Av förarbetena till ovannämnda bestämmelse framgår bland annat följande.

> Första stycket punkten 1 gäller inkomna uppgifter och andra uppgifter som lämnats till myndigheten, t.ex. muntligen. Sådan lag som hänvisas till i punkten 1 är framför allt OSL och förvaltningslagen.
>
> Första stycket punkten 2 ska tolkas så att med handläggning av ett ärende avses detsamma som i förvaltningslagen. I fråga om ett ärende avses alltså något som kännetecknas av att det regelmässigt avslutas genom ett uttalande från myndighetens sida som är avsett att få faktiska verkningar för en mottagare i det enskilda fallet. Ett ärende avslutas således genom ett beslut av något slag.
>
> Första stycket punkten 3 är inte avsedd att tillämpas slentrianmässigt i myndighetens löpande verksamhet. Det krävs att den personuppgiftsansvarige, i det enskilda fallet, gör en bedömning av om behandlingen innebär ett otillbörligt intrång i den registrerades personliga integritet. Om behandlingen skulle innebära ett sådant intrång, får den inte ske enligt denna bestämmelse. För att avgöra om intrånget är otillbörligt måste myndigheten göra en proportionalitetsbedömning där behovet av att utföra behandlingen viktas mot de registrerades intresse av att behandlingen inte sker. Bedömningen av de registrerades intresse av att behandlingen inte sker bör utgå från det intresse av integritetsskydd som de registrerade typiskt sett har. Den personuppgiftsansvarige måste således inte göra en bedömning i förhållande till varje berörd individ. Vid bedömningen av intrånget i den enskildes personliga integritet ska vikt läggas vid bl.a. uppgifternas känslighet, behandlingens karaktär, den inställning de registrerade kan antas ha till behandlingen, den spridning uppgifterna kan komma att få och risken för vidarebehandling för andra ändamål än insamlingsändamålet. Detta innebär t.ex. att bestämmelsen inte kan läggas till grund för att skapa integritetskänsliga sammanställningar av känsliga personuppgifter. Ju mindre tydligt myndighetens behov av att behandla uppgifterna är, desto större är sannolikheten för att de registrerades intresse typiskt sett väger tyngre och att intrånget därför bör betraktas som otillbörligt.
>
> Andra styckets sökbegränsning omfattar alla tekniska åtgärder som innebär att uppgifter används för att strukturera eller systematisera information i syfte att få fram ett urval av personer grundat på känsliga personuppgifter. Därmed förbjuds sökningar som görs för att få fram ett urval av personer som t.ex. har en viss politisk åsikt, religiös åskådning eller sexuell läggning. Däremot hindrar bestämmelsen inte sökningar som görs i ett annat syfte

> än att identifiera ett urval av individer, t.ex. för att utöva tillsyn, för att ta fram verksamhetsstatistik eller för registervård.[35]

Vidare framgår det av förarbetena att behandling av känsliga personuppgifter kan ske med stöd av artikel 9.2 g i dataskyddsförordningen även i andra fall än vad som regleras i dataskyddslagen, under förutsättning att lämpliga och särskilda åtgärder fastställts.[36]

4.4. IMY:s kommentarer

Inledningsvis kan det konstateras att regleringen inte ger något tydligt svar på frågan om i vilken utsträckning tekniska hjälpmedel kan användas för att underlätta hanteringen av begäranden av allmänna handlingar. Det finns därför ett behov av att ge vägledning kring hur sådana hjälpmedel, inklusive AI-baserade verktyg, kan användas i dessa sammanhang.

Maskeringstjänsten

Allmänt om rättslig grund

Den rättsliga grund som kommunen kan stödja användningen av maskeringstjänsten på är uppgift av allmänt intresse (artikel 6.1 e i dataskyddsförordningen).

Regleringen om offentlighetsprincipen i 2 kap. TF ger bland annat kommuner uppgiften att lämna ut allmänna handlingar till den som begär det. Detta är en uppgift av allmänt intresse. Vidare innebär regleringen om sekretess i OSL att bland annat kommuner ska bedöma om uppgifter i allmänna handlingar omfattas av sekretess. Detta innebär att kommuner behöver granska handlingar som omfattas av en begäran och säkerställa att sekretessbelagda uppgifter inte lämnas ut. Även detta utgör en uppgift av allmänt intresse. Hantering av begäranden av allmänna handlingar och sekretessbedömning är således uppgifter av allmänt intresse för kommunen. Dessa uppgifter är fastställda i nationell rätt genom 2 kap. TF och OSL på det sätt som krävs enligt artikel 6.3 i dataskyddsförordningen.

IMY:s bedömning är vidare att regleringen i 2 kap. TF och OSL i princip är tillräckligt tydlig och precis för att ligga till grund för personuppgiftsbehandling i digitala verktyg som underlättar hanteringen av begäranden av allmänna handlingar och sekretessbedömningar. Det gäller till exempel digitala verktyg som används för att manuellt markera uppgifter som omfattas av sekretess. I sådana fall är också dataskyddsförordningens krav på nödvändighet och proportionalitet typiskt sett uppfyllda. När det gäller digitala stöd som innebär en mer omfattande eller riskfylld personuppgiftsbehandling krävs dock en mer ingående bedömning av nödvändighet och proportionalitet för att avgöra om behandlingen är tillåten.

Lidingö stad har uppgett att det finns betydande effektivitetsvinster att göra genom att låta maskeringstjänsten ge stöd vid sekretessbedömningar. IMY konstaterar att om behandlingen leder till sådana effektivitetsvinster kan detta innebära att behandlingen uppfyller nödvändighetskravet i artikel 6.1 e i dataskyddsförordningen.

Vidare kan felaktiga sekretessbedömningar leda till allvarliga konsekvenser för den som berörs. Maskeringstjänsten är dock ett handläggarstöd som förutsätter att det,

[35] Prop. 2017/18:105 s. 194 f, även s. 86–91.
[36] Prop. 2017/18:105 s. 91, jfr s. 84.

utifrån det underlag som tjänsten producerar, ska ske en sekretessprövning av en handläggare. Det har inte framkommit något i projektet som tyder på att maskeringstjänsten i egenskap av ett sådant handläggarstöd skulle medföra några kvalitetsförluster vid sekretessprövningen. Utifrån vad som framkommit i projektet framstår det därmed som att riskerna med behandlingen av personuppgifter i maskeringstjänsten är jämförliga med de risker som uppkommer vid en sekretessbedömning som utförs av en handläggare med hjälp av ett manuellt digitalt maskeringsverktyg. Detta talar för att behandlingen uppfyller kravet på proportionalitet.

Sammantaget innebär detta att det finns mycket som talar för att det finns stöd för behandlingen i artikel 6.1 e i dataskyddsförordningen.

Känsliga personuppgifter

Enligt IMY ger bestämmelserna i 2 kap. TF och OSL, i linje med vad som angetts ovan, uttryck för ett viktigt allmänt intresse som fastställts i nationell rätt. För att bestämmelserna ska kunna utgöra stöd för att behandla känsliga personuppgifter krävs enligt artikel 9.2 g i dataskyddsförordningen att regleringen innehåller sådana lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen. Enligt IMY bör regleringen i 2 kap. TF och OSL ses som en helhet där regleringen om sekretess är en skyddsåtgärd som i sig kan medföra att det finns tillräckligt stöd för att behandla känsliga personuppgifter i samband med sekretessbedömning av allmänna handlingar. Detta förutsätter dock att den skyddsåtgärd som sekretessregleringen innebär är lämplig i förhållande till riskerna med behandlingen. Det krävs naturligtvis också att övrig reglering i dataskyddsförordningen följs, till exempel regleringen om säkerhet i artikel 32. IMY bedömer att den skyddsåtgärd som sekretessregleringen innebär typiskt sett kan vara tillräcklig för den behandling av personuppgifter som sker till exempel i digitala maskeringsverktyg som används för att manuellt markera sekretesskyddade uppgifter. Det finns, utifrån IMY bedömning om rättslig grund ovan, skäl som talar för att motsvarande bedömning bör göras i fråga om maskeringstjänsten.

Av 3 kap. 3 § första stycket 1 dataskyddslagen framgår vidare att känsliga personuppgifter får behandlas av en myndighet om uppgifterna har lämnats till myndigheten och behandlingen krävs enligt lag. I den mån känsliga personuppgifter har lämnats till[37] kommunen anser IMY att det, med beaktande av ovannämnda lagrum, kan finnas stöd för behandling av känsliga personuppgifter i maskeringstjänsten eftersom en myndighet har en lagstadgad skyldighet att göra en sekretessbedömning i samband med ett utlämnande av en allmän handling.

Beträffande andra uppgifter än sådana som lämnats till kommunen kan stöd för behandlingen istället finnas i 3 kap. 3 § första stycket 2 och 3 dataskyddslagen. Av punkten 2 i aktuellt lagrum framgår att känsliga personuppgifter får behandlas av en myndighet om behandlingen är nödvändig för handläggningen av ett ärende. I och med att sekretessbedömning i den mening som avses i denna rapport (se avsnitt 2.3 ovan) innebär ett faktiskt handlande bör det inte röra sig om handläggning av ett ärende. Detta innebär enligt IMY att 3 kap. 3 § första stycket 2 dataskyddslagen inte kan anses vara tillämplig i detta avseende.

---

[37] Med ”lämnats till” avses i sammanhanget enligt förarbetena uppgifter som finns i handlingar som definieras som inkomna enligt 2 kap. 6 § TF eller lämnas till myndigheten på annat sätt, t.ex. muntligen (prop.2017/18:105 s. 194). I doktrin anges att uppgifterna inte lämnats till myndigheten t.ex. när myndigheten genom (personalens) egna iakttagelser vid t.ex. inspektioner har fått tag i dem (Sören Öman, *Dataskyddsförordningen (GDPR) m.m. – En kommentar*, JUNO version 2B, kommentaren till 3 kap. 3 § första stycket första punkten dataskyddslagen).

I 3 kap. 3 § första stycket 3 dataskyddslagen anges därutöver att känsliga personuppgifter får behandlas även i andra fall, om behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse och inte innebär ett otillbörligt intrång i den registrerades personliga integritet. IMY har svårt att se att den behandling av känsliga personuppgifter som görs med maskeringstjänsten innebär ett sådant intrång. Med beaktande av ovanstående anser IMY att behandlingen i maskeringstjänsten kan vara tillåten enligt 3 kap. 3 § första stycket 3 dataskyddslagen. Denna bestämmelse är dock inte avsedd att tillämpas slentrianmässigt och den personuppgiftsansvarige måste alltid göra en proportionalitetsbedömning i varje enskilt fall.

Sammantaget finns det således mycket som talar för att det finns rättsligt stöd för att behandla känsliga personuppgifter i maskeringstjänsten redan med stöd av regleringen i 2 kap. TF och OSL. Vidare är det mycket som talar för att 3 kap. 3 § första stycket 1 dataskyddslagen ger stöd för behandlingen när uppgifterna har lämnats till kommunen. Om de känsliga personuppgifterna inte har lämnats till kommunen kan stöd finnas i 3 kap. 3 § första stycket 3 dataskyddslagen.

Mycket talar för att rättsligt stöd finns

Sammanfattningsvis anser IMY att mycket talar för att det finns rättsligt stöd för användningen av maskeringstjänsten, men att det krävs noggranna överväganden för att säkerställa att den aktuella personuppgiftsbehandlingen är nödvändig och proportionerlig.

Helhetstjänsten

Vad gäller helhetstjänsten finns liksom för maskeringstjänstenen en fastställd uppgift av allmänt intresse i den mening som avses i artikel 6.1 e i dataskyddsförordningen, nämligen genom 2 kap. TF och OSL. Andra bestämmelser som kan vara av intresse beträffande det rättsliga stödet för helhetstjänsten är 4 kap. 1 § och 6 kap. 6 § OSL. Enligt IMY kan dessa bestämmelser i OSL läsas som att de preciserar och tydliggör att det kan finnas en uppgift av allmänt intresse att ge enskilda möjligheter att söka efter allmänna handlingar när den tekniska utvecklingen tillåter det.

Tekniskt kan noteras att helhetstjänsten förutsätter att kommunens diarier kopieras till en separat databas där informationen vektoriseras och indexeras. Därtill måste uppgifterna i diarierna bearbetas kontinuerligt för att kunna identifiera samband, utföra sannolikhetsanalyser och dra slutsatser. Utan helhetstjänsten behandlas dessa uppgifter istället främst genom statisk lagring i arkivsyfte. Den mer avancerade behandling som helhetstjänsten medför ökar generellt sett riskerna för den personliga integriteten. Särskilt är det svårt att förutse risker för den personliga integriteten i förhållande till så kallade potentiella handlingar enligt 2 kap. 6 § andra stycket TF, det vill säga för det fall att helhetstjänsten medför att det blir en rutinbetonad åtgärd i den bestämmelsens mening att använda aktuell teknik. Andra tänkbara risker är att helhetstjänsten vid sökning missar relevanta handlingar eller inkluderar irrelevanta handlingar. Dessa risker kan mildras till exempel genom att man låter handläggare granska det som helhetstjänsten tar fram för utlämning, men i så fall kan det frågas hur noggrann en sådan granskning behöver vara och om resultatet är effektivt och proportionerligt.

Vidare är IMY tveksam till att bestämmelserna i 2 kap. TF och OSL fastställer sådana lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen som krävs enligt artikel 9.2 g i dataskyddsförordningen för

behandling av känsliga personuppgifter i helhetstjänsten. Någon registerförfattning som kan utgöra stöd för behandlingen av känsliga personuppgifter finns heller inte. Behandlingen behöver därför stöd i annan lagstiftning.

I fråga om 3 kap. 3 § första stycket 3 dataskyddslagen anges i förarbetena att integritetskänsliga sammanställningar av känsliga personuppgifter inte har stöd i bestämmelsen. IMY anser att helhetstjänstens separata vektoriserade och indexerade databas kan utgöra en sådan integritetskänslig sammanställning som avses i förarbetena. Det kan också tänkas att behandlingen är sådan som registrerade typiskt sett har ett integritetsintresse av att bli skyddade mot på grund av till exempel riskerna förknippade med potentiella handlingar. Detta talar också för att behandlingen medför otillbörliga risker i bestämmelsens mening.

Vidare kan förbudet i 3 kap. 3 § andra stycket dataskyddslagen tänkas träffa helhetstjänsten med hänvisning till möjligheten att begära potentiella handlingar med sammanställningar av känsliga personuppgifter. I det fallet kan tänkas att den så kallade begränsningsregeln blir tillämplig (se 2 kap. 7 § TF), vilket kan medföra behov av skönsmässiga bedömningar i det enskilda fallet. Det kan frågas om denna skyddsåtgärd kan byggas in i helhetstjänsten (jämför artikel 25 i dataskydds-förordningen) eller om handläggare igen behöver granska resultatet och hur noggrann en sådan granskning behöver vara. Det är oklart om resultatet blir effektivt och proportionerligt i slutändan.

Sammanfattningsvis bedömer IMY att det finns betydande osäkerheter kring helhetstjänstens förenlighet med dataskyddsförordningens nödvändighets- och proportionalitetsprinciper. Den rättsliga grunden, som utgörs av allmänt hållna bestämmelser i TF och OSL, är inte tillräckligt förutsebar och preciserad i relation till de risker som finns för den personuppgiftsbehandling som sker i samband med användningen av helhetstjänsten. Därför bedöms de potentiella konsekvenserna för den personliga integriteten vara för otydliga och kan inte säkerställas som proportionerliga. Sammantaget anser alltså IMY att övervägande skäl talar för att den personuppgiftsbehandling som sker i samband med användningen av helhetstjänsten saknar rättslig grund i dagsläget.

5. Hur fördelas personuppgiftsansvaret?

5.1. Vad är personuppgiftsansvar?

Med personuppgiftsansvarig avses, enligt artikel 4.7 i dataskyddsförordningen, en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Begreppet personuppgiftsansvarig ska enligt EU-domstolen tolkas brett. Syftet med en bred definition är att säkerställa ett effektivt och komplett skydd för de registrerade.[38] Definitionen omfattar varje organ som ensamt eller tillsammans med andra bestämmer ändamål och medel.[39] EDPB har i riktlinjerna 07/2020 om begreppen ”personuppgiftsansvarig” och ”personuppgiftsbiträde” uttalat att det i praktiken är en organisation och inte en person inom organisationen som är personuppgiftsansvarig.[40]

Personuppgiftansvaret ska enligt EDPB bedömas utifrån de faktiska och relevanta omständigheterna som råder i det enskilda fallet.[41] Avgörande för denna bedömning är bland annat varför behandlingen utförs och vem som är initiativtagare till behandlingen. Rekvisiten ändamål och medel kan förstås som *varför*, det vill säga i vilket syfte, något ska utföras och *hur* något ska utföras för att syftet ska uppnås. Av den så kallade ändamålsprincipen i artikel 5.1 b i dataskyddsförordningen framgår att personuppgifter bara får samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte får vidarebehandlas på ett sätt som är oförenligt med dessa ändamål. Den personuppgiftsansvarige måste enligt EDPB bestämma både ändamål *och* medel för att personuppgiftsansvar ska utlösas, det alltså inte tillräckligt att enbart bestämma ändamål.[42]

Personuppgiftsansvaret kan också vara utpekat i lag eller förordning, om också ändamålen och medlen bestäms i författningen. Så är exempelvis fallet i de registerförfattningar som finns för offentlig sektor, särskilt när ändamålen för de aktuella behandlingarna av personuppgifter eller registren bestäms i författningen och inte av den aktuella myndigheten. Om en behandling av personuppgifter syftar till att uppfylla ett författningsreglerat krav är det den som har att uppfylla kravet som antas vara personuppgiftsansvarig.[43]

Om den personuppgiftsansvarige brister i efterlevnaden av dataskyddsreglerna kan den bli skadeståndsansvarig enligt dataskyddsförordningen och kompletterande nationell lagstiftning. Av detta följer att det därför bara är sådana organ som har rättskapacitet som kan betraktas som personuppgiftsansvariga.[44]

Gemensamt personuppgiftsansvar

Gemensamt personuppgiftsansvar definieras i artikel 4.7 och artikel 26.1 i dataskyddsförordningen som att två eller fler personuppgiftsansvariga gemensamt

---

[38] EU-domstolen, IAB Europe, C-604/22, EU:C:2024:214, punkt 55.
[39] EU-domstolen, Land Hessen, C-272/19, EU:C:2020:535, punkt 65.
[40] EDPB, Riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR version 2.0, antaget den 7 juli 2021, sida 11.
[41] EDPB, Riktlinjer 07/2020, sida 13 och 20.
[42] EDPB, Riktlinjer 07/2020, sida 12–13, 15 och 20.
[43] Öman S., Dataskyddsförordningen (GDPR) m.m., en kommentar, (2023, version 2B, JUNO), kommentaren till artikel 4.1 punkt 7.
[44] Öman S., Dataskyddsförordningen (GDPR) m.m., en kommentar, (2023, version 2B, JUNO), kommentaren till artikel 4.1 punkt 7.

fastställer ändamålen med och medlen för behandlingen. EDPB har uttalat att gemensamt ansvar kan uppstå när flera parter är inblandade, men att all behandling där flera parter är inblandade inte innebär gemensam kontroll. Gemensam kontroll föreligger enligt EDPB när parter som är involverade i samma behandling utför behandlingen för samma eller gemensamma ändamål. Ändamålen kan vara nära sammankopplade *eller* kompletterande. Så kan fallet vara om de involverade parterna drar ömsesidig nytta av samma behandling, förutsatt att samtliga parter deltar i fastställande av ändamål och medel.[45]

Av EU-domstolens praxis framgår att fastställande av ändamål och medel kan ske antingen genom ett gemensamt beslut eller genom ett så kallat konvergerande beslut från två eller flera parter. Med konvergerande beslut avses beslut som kompletterar varandra och är nödvändiga för att behandlingen ska ske på ett sådant sätt att de har en påtaglig inverkan på fastställandet av behandlingens ändamål och behandlingssätt. Det ska då inte vara möjligt att skilja parternas behandling från varandra. [46]

EU-domstolen har i tidigare avgöranden slagit fast att det är tillräckligt att en aktör, för sina egna ändamål, påverkar behandlingen för att anses ha deltagit i bestämmande av ändamål och medel och därmed anses gemensamt ansvarig för behandlingen. Det krävs inte att var och en av parterna har tillgång till uppgifterna för att gemensamt ansvar ska uppstå,[47] utan det är tillräckligt att en part har haft ett väsentligt inflytande på behandlingen.[48] Det krävs heller inte att båda parterna utför själva behandlingen för att ett gemensamt ansvar ska uppstå, utan det är tillräckligt att en part möjliggör behandlingen[49] eller har varit den som organiserat, samordnat och uppmuntrat till behandlingen.[50] Av EU-domstolens avgöranden framgår också att gemensamt ansvar inte nödvändigtvis behöver innebära likvärdigt ansvar, varpå olika aktörer kan vara involverade i olika skeden och i olika utsträckning.[51] En gemensam personuppgiftsansvarig kan enligt EU-domstolen inte anses vara ansvarig för tidigare eller senare åtgärder i behandlingskedjan som denne varken fastställt ändamål eller medel för.[52]

När ett gemensamt ansvar föreligger är alla parter var och en ansvariga för att se till att behandlingen följer dataskyddsreglerna. Exempelvis är vardera part skyldig att säkerställa att den har en rättslig grund för behandlingen och att personuppgifterna inte vidarebehandlas på ett sätt som är oförenligt med ändamålet för vilket informationen ursprungligen samlades in av den personuppgiftsansvarige.

EDPB ger i sin vägledning flera exempel på när ett gemensamt ansvar kan uteslutas. Gemensamt ansvar föreligger exempelvis inte i situationer där två parter delar personuppgifter men saknar gemensamt ändamål. Att en part enbart drar nytta av en behandling, till exempel en kommersiell sådan, ger enligt EDPB inte upphov till gemensamt ansvar. Om en part inte har något eget syfte i förhållande till behandlingen, utan bara tillhandahåller tjänster mot betalning, fungerar den parten som ett personuppgiftsbiträde snarare än som en gemensam personuppgiftsansvarig. Gemensamt ansvar kan även uteslutas i fall där flera aktörer använder en gemensam

[45] EDPB, Riktlinjer 07/2020, sida 21–22 och 26.
[46] EU-domstolen, IAB Europe, C-604/22, ECLI:EU:C:2024:214, punkt 59.
[47] EU-domstolen, IAB Europe, C-604/22, EU:C:2024:214, punkterna 57–58. Se även EU-domstolens dom den 29 juli 2019, Fashion ID, C-40/17, ECLI:EU:2018:1039, punkt 69.
[48] EU-domstolen, Fashion ID, C-40/17, ECLI:EU:2018:1039, punkterna 78–79. Se även liknande resonemang EU-domstolen, Belgian State, C-231/22, EU:C:2024:7, punkt 48.
[49] EU-domstolen, Wirtschaftsakademie Schleswig-Holstein GmbH, C-210/16, EU:C:2018:388, punkterna 36–39.
[50] EU-domstolen, Jehovan todistajat, C-25/17, EU:C:2018:551, punkt 73.
[51] EU-domstolen, IAB Europe, C-604/22, ECLI:EU:C:2024:214, punkt 58.
[52] EU-domstolen, IAB Europe, C-604/22, ECLI:EU:C:2024:214, punkt 73.

databas eller infrastruktur men varje aktör självständigt fastställer sina egna ändamål. I synnerhet i de fall där aktörernas behandling går att hålla isär och kan utföras av en aktör utan ingripande från en annan.[53]

Datadelningsavtal

I artikel 26 i dataskyddsförordningen anges att gemensamt personuppgiftsansvariga under öppna former ska fastställa sitt respektive ansvar och komma överens om sina respektive ansvarsområden för efterlevnad av förordningens krav. Ett sådant arrangemang kallas ofta för datadelningsavtal. Det finns inga formkrav för hur detta ska ske, men EDPB:s rekommendation är att det görs i form av ett bindande dokument, såsom ett avtal eller en annan juridiskt bindande handling.[54]

Syftet med att reglera ansvaret är att undvika kryphål där vissa skyldigheter inte efterlevs av någon av parterna.[55] Av praxis från EU-domstolen framgår dock att ansvaret inte behöver vara lika fördelat mellan de gemensamt personuppgiftsansvariga.[56]

Oavsett vad parterna avtalat om har de registrerade, enligt artikel 26.3 i dataskyddsförordningen, rätt att vända sig till var och en av de personuppgiftsansvariga för att utöva sina rättigheter. Enligt artikel 82.5 i förordningen har en personuppgiftsansvarig som betalat skadeersättning till en registrerad rätt att kräva övriga ansvariga på deras respektive andelar av ersättningen, i proportion till deras ansvar för skadan.[57]

Tillsynsmyndigheterna är inte bundna av parternas avtalade ansvarsfördelning. De har rätt att utöva tillsyn, eller använda någon av sina andra befogenheter, gentemot vilken som helst av de gemensamt personuppgiftsansvariga.[58]

Personuppgiftsbiträden

Med personuppgiftsbiträde avses, enligt artikel 4.8 i dataskyddsförordningen, en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Enligt EDPB ska bestämmelsen förstås som att den personuppgiftsansvarige har delegerat hela eller delar av behandlingen till en extern aktör utanför den egna organisationen. Exempelvis kan ett företag inom en koncern vara biträde till ett annat företag inom samma koncern, men olika avdelningar inom ett och samma företag kan däremot inte vara biträde åt varandra.[59]

För att det ska vara fråga om en biträdessituation ska det vara den personuppgiftsansvarige som har bestämt ändamål och medel. Personuppgiftsbiträdet har inget inflytande över behandlingens ändamål eller behandlingsmedlen utan får endast behandla personuppgifter efter den personuppgiftsansvariges instruktioner. Det framgår av artikel 28.10 i dataskyddsförordningen att om personuppgiftsbiträdet

[53] EDPB, Riktlinjer 07/2020, sida 23 och 26.
[54] EDPB, Riktlinjer 07/2020, sida 50.
[55] EDPB, Riktlinjer 07/2020, sida 47.
[56] EU-domstolen, Wirtschaftsakademie Schleswig-Holstein GmbH, C-210/16, EU:C:2018:388, punkt 43.
[57] Se även 7 kap. 1 § dataskyddslagen.
[58] EDPB, Riktlinjer 07/2020, sida 52.
[59] EDPB, Riktlinjer 07/2020, sida 28.

fastställer egna ändamål och medel blir personuppgiftsbiträdet ansvarig för den behandlingen. EDPB menar att det av detta följer att en aktör kan vara både personuppgiftsansvarig och personuppgiftsbiträde samtidigt, om aktören utför behandling på uppdrag av annan aktör samt behandlar personuppgifter för egna ändamål. Ett personuppgiftsbiträde har dock viss handlingsfrihet. Exempelvis får biträdet fatta beslut om mer praktiska delar av genomförandet av behandlingen, såsom val av programvara eller val av lämpliga säkerhetsåtgärder. Beslut avseende så kallade väsentliga medel, som är nära kopplade till behandlingens ändamål och omfattning, såsom vilken typ av personuppgifter som behandlas, hur länge uppgifterna ska behandlas, vem som ska ha åtkomst till uppgifterna och vilkas personuppgifter som ska behandlas, får däremot endast beslutas av den personuppgiftsansvarige.[60]

Det framgår vidare av artikel 28.1 att en personuppgiftsansvarig endast får anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i dataskyddsförordningen och säkerställer att den registrerades rättigheter skyddas. Den personuppgiftsansvarige och personuppgiftsbiträdet ska även enligt artikel 28.3 upprätta ett avtal eller annan juridisk handling avseende den personuppgiftsbehandling som biträdet ska utföra, ett så kallat personuppgiftsbiträdesavtal. Det anges i artikel 28.3 vad som ska regleras i avtalet, men avtalet bör enligt EDPB inte bara upprepa dataskyddsförordningens bestämmelser utan snarare inkludera mer specifik och konkret information angående hur kraven ska uppfyllas och vilken säkerhetsnivå som krävs för behandlingen.[61]

När personuppgiftbiträdet upphör med behandlingen som denne utför på uppdrag av den personuppgiftsansvarige måste biträdet radera eller återlämna alla personuppgifter, inklusive eventuella kopior, till den personuppgiftsansvarige. Dock ska personuppgiftsbiträdet behålla uppgifterna om det finns krav på detta enligt EU-rätten eller nationell lagstiftning (artikel 28.3 g i dataskyddsförordningen).

Underbiträden

Ett personuppgiftsbiträde får anlita ett eller flera andra personuppgiftsbiträden, så kallade underbiträden, för delar av behandlingen. Artikel 28.2 i dataskyddsförordningen ställer dock krav på att personuppgiftsbiträdet måste inhämta ett särskilt eller allmänt skriftligt förhandstillstånd från den personuppgiftsansvarige. Med särskilt förhandstillstånd avses enligt EDPB att ett specifikt underbiträde angetts för en specifik behandlingsaktivitet vid en specifik tidpunkt.[62] Av artikel 28.2 framgår att i det fall personuppgiftsbiträdet har erhållit ett allmänt skriftligt tillstånd måste denne informera den personuppgiftsansvarige i rimlig tid om eventuella planer på att anlita ett underbiträde.

Om ett personuppgiftsbiträde anlitar ett underbiträde ska personuppgiftsbiträdet enligt artikel 28.4 ingå ett avtal med underbiträdet i vilket underbiträdet åläggs samma skyldigheter som personuppgiftsbiträdet. Personuppgiftsbiträdet är då fullt ansvarig gentemot den personuppgiftsansvarige för den behandling underbiträdet utför.

---

[60] EDPB, Riktlinjer 07/2020, sida 16 och 28-29.
[61] EDPB, Riktlinjer 07/2020, sida 37.
[62] EDPB, Riktlinjer 07/2020, sida 27 och 45-46.

5.2. IMY:s kommentarer

Hur fördelas ansvaret mellan nämnderna i kommunen?

Lidingö stad styrs av kommunfullmäktige. Under kommunfullmäktige lyder stadens sju nämnder, dit bland annat kommunstyrelsen hör.[63] Lidingö stad har skrivit in i sina reglementen att varje nämnd är personuppgiftsansvarig för de register och andra behandlingar av personuppgifter som sker i nämndernas verksamhet.[64] Nämnderna har huvudsakligen separata diarier[65] och har endast delvis tillgång till varandras diarier och de personuppgifter som förekommer däri. I dagsläget är således nämnderna var och en personuppgiftsansvarig för sina respektive diarier och för den manuella sekretessbedömning och maskering som sker vid en begäran om en allmän handling.

Den fråga som varit föremål för diskussion har varit om nämnderna ska betraktas som separat personuppgiftsansvariga eller som gemensamt personuppgiftsansvariga när de använder maskeringstjänsten.

IMY:s uppfattning har tidigare varit, under tiden då personuppgiftslagen (1998:204) var gällande, att kommunstyrelsen och nämnderna i en kommun, om det är så att det är självständiga förvaltningsmyndigheter, normalt är personuppgiftsansvariga var och en för sig i sin verksamhet. Vilket organ i kommunen som är personuppgiftsansvarig har enligt IMY avgjorts bland annat utifrån om nämnden självständigt förfogar över de personuppgifter som behandlas.[66]

I det aktuella fallet är det kommunstyrelsen som har beslutat att ta fram maskeringstjänsten för ändamålet att effektivisera utlämnandeprocessen av allmänna handlingar inom kommunen. Det är således kommunstyrelsen som är initiativtagare till behandlingen. Det är också kommunstyrelsen som har upphandlat tjänsten och som bestämmer vilka funktioner som tjänsten ska ha. De andra nämnderna är inte delaktiga i den processen.

Tanken är att nämnderna självständigt ska kunna besluta om de vill använda maskeringstjänsten i sin verksamhet eller inte och i så fall för vilka syften. Om nämnderna väljer att använda tjänsten kommer varje nämnd, likt i dagsläget, att behandla uppgifter i deras egna diarium, som nämnderna har eget ansvar för. Det kommer av det skälet vara möjligt att hålla isär nämndernas behandlingar från varandra och behandlingarna kommer ske utan ingripande från någon annan nämnd. Nämnderna kommer därmed att kunna fastställa sina egna ändamål och medel för behandlingen.

Maskeringstjänsten är avsedd att användas som ett handläggarstöd (se avsnitt 3.2 ovan). Det kommer i likhet med den manuella sekretessbedömning och maskering som sker idag vara den enskilda handläggaren som fattar beslut om utlämnande. Det är mycket som talar för att användningen av maskeringstjänsten inte kommer innebära en annan fördelning av personuppgiftsansvaret än vad som har fastställts i Lidingö stads reglementen.

---

[63] Lidingö stad, *Så styrs Lidingö,* tillgänglig: Så styrs Lidingö - Lidingö stad (lidingo.se), uppdaterad senast 2024-04-29.
[64] Lidingö stads reglementen finns tillgängliga på: Så styrs Lidingö - Lidingö stad (lidingo.se), uppdaterad senast 2024-06-18.
[65] Lidingö stad har även ett gemensamt diarium för kommunen.
[66] Datainspektionen, Informationsblad om personuppgiftsansvar, december 2010.

Sammanfattningsvis finner IMY att det finns flera omständigheter som talar för att var och en av nämnderna är separat ansvarig för den personuppgiftsbehandling som sker när maskeringstjänsten används.

Hur fördelas ansvaret mellan nämnderna och tjänsteleverantören?

Kommunstyrelsen hos Lidingö stad har gett tjänsteleverantören Atea i uppdrag att tillhandahålla en AI-tjänst för maskering och sekretessbedömning i syfte att effektivisera utlämnandeprocessen av allmänna handlingar. Detta ändamål har bestämts ensidigt av Lidingö stad utan någon påverkan från Atea. Det är vidare Lidingö stad som är ansvarig för att lämna ut allmänna handlingar och att dessa hanteras effektivt. Dessa omständigheter talar för att det inte finns något gemensamt ändamål för parterna.

Det förefaller heller inte som att Atea har något eget ändamål med behandlingen, eftersom en ren kommersiell fördel inte i sig kvalificerar som ett ändamål.

Det är vidare kommunstyrelsen som bestämmer vilka funktioner som maskeringstjänsten ska ha. Atea lägger därefter fram förslag på olika tekniska lösningar varpå Lidingö stad kan välja de lösningar som bäst uppnår deras ändamål. Enligt IMY finns det indikationer på att det är Lidingö stad som bestämmer medlen för behandlingen. Det förhållande att det är Atea som besitter den tekniska kompetensen och tar fram lösningar behöver inte förändra den bedömningen. Det kan snarare betraktas som ett led i Lidingö stads bestämmande av medel att de valt att anlita Ateas expertis för ändamålet.

Omständigheten att Lidingö stad bestämmer vilka diarier maskeringstjänsten ska ha tillgång till och vilka uppgifter den därmed ska behandla talar också för att det är Lidingö stad som bestämmer de väsentliga medlen för behandlingen. I synnerhet om också Lidingö stad bestämmer över hur länge uppgifterna får sparas och vilka som ska ha åtkomst till uppgifterna som kommer att behandlas av maskeringstjänsten.

När maskeringstjänsten är driftsatt är planen att behandlingen av data ska ske dels lokalt hos Lidingö stad, dels i Ateas datacenter. Atea kommer då att ha tillgång till de uppgifter som behandlas i bolagets datacenter. I det fall att Atea då skulle kunna ändra eller radera uppgifterna kan det tala för att Atea har ett gemensamt ansvar tillsammans med Lidingö stad för den behandling som sker i bolagets datacenter. Om tjänsten däremot sätts upp så att Atea endast ansvarar för driften, men inte kan utöva någon kontroll över uppgifterna, talar det å andra sidan för att Atea snarare har ett renodlat biträdesansvar.[67]

Sammanfattningsvis finner IMY att det finns flera omständigheter som talar för att Atea är att betrakta som personuppgiftsbiträde för den behandling av personuppgifter som sker när makeringstjänsten används. Detta skulle i så fall innebära att Atea inte är ansvarig gentemot de registrerade så länge de följer de instruktioner som de fått av Lidingö stad. Skulle Atea däremot vilja använda de personuppgifter som maskeringstjänsten samlar in för att exempelvis träna eller ta fram nya maskeringstjänster eller liknande, kommer det att betraktas som en ny behandling som också Atea ansvarar för.

[67] IMY har tidigare, under den då gällande personuppgiftslagen, fört ett liknande resonemang om att en användare som enbart har rätt att komma åt personuppgifter genom att läsa dem och söka bland dem men som inte självständigt får ändra, komplettera eller radera uppgifterna inte är personuppgiftsansvarig. Se Datainspektionen, Informationsblad om personuppgiftsansvar, december 2010.

6. Vad kan vara lämpliga säkerhetsåtgärder vid användningen av AI-tjänsten?

6.1. Säkerhet i samband med behandlingen

Artikel 32 i dataskyddsförordningen handlar om säkerheten vid behandling av personuppgifter och ställer krav på att både personuppgiftsansvariga och personuppgiftsbiträden ska säkerställa en adekvat skyddsnivå för de personuppgifter som behandlas. Syftet är bland annat att skydda personuppgifter från obehörig åtkomst, förlust, ändring eller annan olaglig behandling.

Enligt artikel 32 ska lämpliga tekniska och organisatoriska åtgärder vidtas för att säkerställa en säkerhetsnivå som är anpassad till risken med behandlingen. Bedömningen av säkerhetsåtgärdernas lämplighet ska ske med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter. Efterlevnaden av artikel 32 innebär en kontinuerlig process där personuppgiftsansvariga och personuppgiftsbiträden måste utvärdera och justera sina säkerhetsåtgärder i takt med förändringar i riskbilden och den tekniska utvecklingen.

Riskbedömning

Riskbedömningen är enligt artikel 32 i dataskyddsförordningen en central del för att säkerställa att säkerhetsåtgärderna vid behandlingen är adekvata och proportionerliga. Syftet med riskbedömningen är att identifiera och analysera potentiella hot mot personuppgifternas säkerhet och de registrerades rättigheter och friheter och därefter fastställa vilka åtgärder som krävs för att hantera dessa risker. Riskbedömningen bör följa hela livscykeln för personuppgiftsbehandlingen och ta hänsyn till de specifika riskerna som aktualiseras samt sannolikheten för att en säkerhetsincident inträffar, liksom den potentiella skada som en sådan incident skulle kunna orsaka de registrerade.

Vid genomförandet av en riskbedömning bör flera faktorer övervägas. Hänsyn bör bland annat tas till typen av personuppgifter som behandlas. Känsliga personuppgifter medför högre risker och kräver därmed starkare skyddsåtgärder. Även omfattningen och syftet med behandlingen bör beaktas, då storskalig eller automatisk behandling kan innebära högre risker. Dessutom bör den tekniska miljön uppmärksammas, inklusive sårbarheter i it-systemen, samt de organisatoriska strukturerna och processerna som är på plats för att skydda uppgifterna. Efter att ha identifierat och analyserat riskerna bör den personuppgiftsansvarige besluta om lämpliga tekniska och organisatoriska åtgärder, såsom rutiner, utbildning, kryptering, åtkomstkontroller och kontinuerlig övervakning, för att minimera de identifierade riskerna.

Identifiering av risker kan vara krävande och svårt när det gäller användningen av ny teknik som kräver specifika kunskaper inom organisationen. Användningsområden och möjligheterna med ny teknik, såsom AI, utvecklas snabbt. Att hålla organisationen uppdaterad om potentiella risker, möjliga åtgärder eller nya normer inom branschen kan vara tidskrävande om rätt resurser saknas. Att skapa förutsättningar som möjliggör identifiering av risker är avgörande för att uppnå en heltäckande riskbedömning.

6.2. Lämpliga organisatoriska och tekniska säkerhetsåtgärder

Organisatoriska säkerhetsåtgärder syftar till att minska risker på ett rent organisatoriskt, systematiskt och administrativt plan i förhållande till personuppgiftsbehandlingen. Sådana åtgärder kan exempelvis omfatta interna rutiner, instruktioner och riktlinjer, liksom inrättandet av tydliga åtkomsträttigheter och utbildningsprogram för att höja medvetenheten och förståelsen hos personalen, exempelvis vad som ligger till grund för slutsatser gjorda av AI-modeller eller vilka risker som finns med användningen.

Tekniska säkerhetsåtgärder är åtgärder som kan kopplas till att minska risker på ett tekniskt plan, exempelvis kryptering, pseudonymisering, säkerhetskopiering, skydd mot virus och möjlighet att upptäcka sårbarheter och angrepp på system som används i personuppgiftsbehandlingen.

Både tekniska och organisatoriska säkerhetsåtgärder är nödvändiga att implementera vid behandling av personuppgifter. Den personuppgiftsansvarige är ytterst ansvarig för att säkerhetsåtgärderna är tillräckliga, men den personuppgiftsansvarige och personuppgiftsbiträdet ska tillsammans vidta åtgärder för att säkerställa att skyddet för personuppgifter upprätthålls. Personuppgiftsbiträdet har också ett visst utrymme att fastställa ”icke-väsentliga medel” gällande särskilda praktiska aspekter av implementeringen av personuppgiftsbehandlingen, såsom valet av maskin- eller programvara eller detaljerade säkerhetsåtgärder i det enskilda fallet.[68] Personuppgiftsbiträdet ska kunna ge tillräckliga garantier, i synnerhet i fråga om sakkunskap, tillförlitlighet och resurser, för att genomföra tekniska och organisatoriska åtgärder som är lämpliga i förhållande till risken med behandlingen.

Att besitta rätt kompetens är av stor vikt för att kunna identifiera riskerna vid användningen av AI och bedöma vilka säkerhetsåtgärder som är lämpliga. Det pågår flera initiativ för att göra det enklare att identifiera de tekniska och organisatoriska riskerna som finns inom området. Många tillverkare av språkmodeller delar information om modellens prestanda, styrkor och svagheter samt hur de hanterat kända sårbarheter. Under 2024 publicerade forskare vid MIT rapporten AI Risk Repository som är en sammanställning av mer än 700 kända riskområden inom AI.[69] Databasen är tänkt att bistå organisationer med identifiering och förståelse av eventuella risker. Vidare har Digg tagit fram den så kallade Förtroendemodellen som är ett användbart verktyg för självutvärdering vid användning av AI.[70] Förtroendemodellen kan med fördel användas av offentliga verksamheter för att säkerställa att AI används på rätt sätt i den egna organisationen.

[68] EDPB, Riktlinjer 07/2020, sida 16.
[69] AI Risk Repository (https://airisk.mit.edu).
[70] Digg, Förtroendemodellen för artificiell intelligens (https://www.dataportal.se/fortroendemodellen).

6.3. Konsekvensbedömning

Om den personuppgiftsbehandling som planeras sannolikt förväntas leda till hög risk för registrerades rättigheter och friheter behöver den personuppgiftsansvarige genomföra en konsekvensbedömning enligt artikel 35 i dataskyddsförordningen. Syftet är att utreda den planerade behandlingens konsekvenser för skyddet av personuppgifterna. Konsekvensbedömningen går ett steg längre än riskbedömningen och innehåller bland annat också en bedömning av hur den tilltänkta behandlingen lever upp till de grundläggande laglighetskraven samt kraven på nödvändighet och proportionalitet för behandlingen. I artikel 35.3 i dataskyddsförordningen anges vissa situationer när en konsekvensbedömning alltid krävs, om inte undantaget i artikel 35.10 är tillämpligt. Utöver det har också IMY, med ledning av riktlinjer från EDPB och de kriterier som detta organ fastställt, antagit en förteckning över ytterligare behandlingar som kräver en konsekvensbedömning.[71] Förteckningen är inte uttömmande och kan komma att uppdateras och kompletteras med fler exempel framöver.

Utöver de situationer som anges i artikel 35.3, och med beaktandet av undantaget i artikel 35.10, ska en konsekvensbedömning avseende dataskydd göras om den planerade behandlingen uppfyller minst två av följande kriterier:

1. utvärderar eller poängsätter människor, till exempel ett företag som erbjuder genetiska tester till konsumenter för att bedöma och förutse risker för sjukdomar, ett kreditupplysningsföretag eller ett företag som profilerar internetanvändare
2. behandlar personuppgifter i syfte att fatta automatiserade beslut som har rättsliga följder eller liknande betydande följder för den registrerade
3. systematiskt övervakar människor, till exempel genom kameraövervakning av en allmän plats eller genom att samla in personuppgifter från internetanvändning i offentliga miljöer
4. behandlar känsliga personuppgifter enligt artikel 9 eller uppgifter som är av mycket personlig karaktär, till exempel ett sjukhus som lagrar patientjournaler, ett företag som samlar in lokaliseringsuppgifter eller en bank som hanterar finansiella uppgifter
5. behandlar personuppgifter i stor omfattning
6. kombinerar personuppgifter från två eller flera behandlingar på ett sätt som avviker från vad de registrerade rimligen kunnat förvänta sig, till exempel när man samkör register
7. behandlar personuppgifter om personer som av något skäl befinner sig i ett underläge eller i beroendeställning och därför är sårbara, till exempel barn, anställda, asylsökande, äldre och patienter
8. använder ny teknik eller nya organisatoriska lösningar, till exempel en sakernas internet-applikation (Internet of things, IoT)
9. behandlar personuppgifter i syfte att hindra registrerade från att få tillgång till en tjänst eller ingå ett avtal, till exempel när en bank granskar sina kunder mot en databas för kreditupplysning för att besluta om de ska erbjudas lån.

En konsekvensbedömning ska genomföras innan den tilltänkta behandlingen påbörjas. Det är möjligt att en personuppgiftsansvarig bedömer att personuppgiftsbehandlingen

[71] Artikel 29-gruppen, Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679, 17/SV, WP 248 rev. 01, antaget den 4 april 2017 och reviderat den 4 oktober 2017, s. 10 ff. samt IMY:s förteckning över när en konsekvensbedömning ska göras (https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/konsekvensbedomningar-och-forhandssamrad/forteckning-over-nar-en-konsekvensbedomning-ska-goras/).

sannolikt inte leder till hög risk för registrerade trots att behandlingen uppfyller två eller flera av ovanstående kriterier. I sådana situationer bör den personuppgiftsansvarige motivera och dokumentera skälen till att en konsekvensbedömning inte utförs. Om organisationen har ett dataskyddsombud ska ombudet rådfrågas. Dokumentationen bör inkludera dataskyddsombudets synpunkter.

6.4. IMY:s kommentarer

Tekniska och organisatoriska säkerhetsåtgärder kopplat till användning av AI kräver både anpassning till mängden och karaktären hos personuppgifterna som avses att behandlas, men också till egenskaper som är unika för den tilltänkta AI-tjänsten. Det kan också finnas redan implementerade säkerhetsåtgärder i en förtränad modell som skiljer sig åt mellan olika tillverkare och språkmodeller som kan vara nödvändiga att utvärdera. De lämpliga säkerhetsåtgärder som diskuteras i denna del av rapporten ska inte ses som en uttömmande uppräkning över de säkerhetsåtgärder som bör övervägas vid införandet av AI i en organisation. Inte heller beaktas det vilka säkerhetsåtgärder som kan vara nödvändiga i förhållande till själva utvecklingen av AI, eftersom projektet som är föremål för den här rapporten avser användning av en redan färdigtränad AI-modell.

I fall som det förevarande där Lidingö stad önskar att använda en maskeringstjänst som genom språkmodeller identifierar personuppgifter i handlingar samt lämnar förslag på vilka uppgifter som kan omfattas av sekretess kan särskilda risker bestå i att handläggaren i för stor utsträckning förlitar sig på AI-modellens bedömningar. Det kan leda till att exempelvis uppgifter som ska vara sekretessbelagda ändå lämnas ut eller att uppgifter som ska lämnas ut trots allt beläggs med sekretess. Andra risker relaterar till data som överförs till tredje part som skulle kunna innebära en ökad risk för att personuppgifter kommer obehöriga tillhanda. För att hantera denna typ av risker anser IMY att följande säkerhetsåtgärder särskilt bör övervägas:

- **Styrning**: Etablera en tydlig styrningsstruktur med definierade roller och ansvarsområden kopplat till AI-användningen vilken kommuniceras inom organisationen. Detta inkluderar att skapa policy och rutiner för användningen av AI som beaktar hela AI-tjänstens livscykel. Dokumenten bör vara skriftliga och allmänt tillgängliga inom organisationen samt fortlöpande omprövas för att anpassas till aktuellt behov av säkerhet.

- **Mänsklig kontroll** (eng. *human-in-the-loop*): För verksamheter som planerar att använda en färdigtränad AI-modell innebär det att modellen kommer att kunna reproducera likvärdiga resultat över tid, men stora variationer kan ändå förekomma. En tydlig ansvarsstruktur och uppföljningsprocess för AI-modellens resultat bör etableras innan tjänsten tas i bruk. Likt andra AI-baserade tjänster kommer maskeringstjänsten inte att fungera helt felfritt. Det kommer alltid att finnas en viss felmarginal som innebär att tjänsten ibland kommer att göra misstag i sina sekretessbedömningar. Det är viktigt att de handläggare som ska använda maskeringstjänsten utbildas om detta och förstår hur AI-modellen på ett övergripande plan har resonerat för att komma fram till sin slutsats. Vidare är det viktigt att handläggarna är medvetna om AI-tjänstens förmågor och begränsningar för att undvika en övertro till tjänstens kapacitet. Maskeringstjänsten ska endast betraktas som ett arbetsstöd och handläggarna behöver alltid noggrant granska dess resultat för att säkerställa att sekretessbedömningen blir korrekt i slutändan.

- **Kryptering**: Stark kryptering bör användas för personuppgifter som överförs till en extern leverantör, både vid överföring och lagring av data. Detta minskar

risken för obehörig åtkomst i händelse av ett säkerhetsintrång eller vid oavsiktlig exponering av personuppgifterna eftersom krypteringen gör informationen oläslig för obehöriga parter. När maskeringstjänsten sätts i drift blir det viktigt att säkerställa att personuppgifterna är skyddade i samband med att de överförs och behandlas hos Atea som extern leverantör.

Utöver ovanstående kan även följande åtgärder övervägas i relation till användning av AI-tjänster:

- **Begränsa språkmodellen**: Begränsa språkmodellens funktionalitet till att endast kunna utföra det som är relevant för syftet med den specifika tjänsten. Det kan bland annat ske genom att begränsa möjliga kommandon som användaren kan ge till modellen eller skapa begränsande instruktioner. Säkerställ att språkmodellen inte utför nya instruktioner som skulle kunna förekomma i den text som tjänsten är avsedd att hantera. Minimera mängden data genom att AI-tjänsten endast får tillgång till de uppgifter som är nödvändiga för ändamålet med behandlingen. På så sätt begränsas omfattningen av potentiella skador vid en eventuell dataläcka.

- **Utvärdera organisationen**: Utvärdera mognaden för AI i organisationen samt den acceptabla användningen utifrån organisationens riskprofil och hur det kan påverka användningen av en AI-tjänst eller dess komponenter. Bredare insatser, såsom utbildningsprogram, resursallokering och tvärfunktionellt samarbete mellan olika team är av stor vikt för att minska risker när en AI-tjänst tas i drift i verksamheten.

- **Kontrollera personuppgiftsbiträden**: Etablera kontroll över leverantörskedjan kopplat till AI, särskilt när en eller flera externa parter är inblandade, exempelvis när AI-modellen körs på externa servrar eller i molnet. Parter som utgör personuppgiftsbiträden och underbiträden behöver kunna garantera säkerheten för de personuppgifter som behandlas och den personuppgiftsansvarige behöver se till att avtalsenliga förpliktelser har etablerats i enlighet med artikel 28 i dataskyddsförordningen, inklusive nödvändiga sekretessförbindelser. Det är också den personuppgiftsansvarige som ansvarar för att skyldigheterna avseende inbyggt dataskydd och dataskydd som standard enligt artikel 25 i dataskyddsförordningen fullgörs vid den behandling som utförs av deras personuppgiftsbiträden och underleverantörer. Därför bör personuppgiftsansvariga särskilt ta hänsyn till hur detta efterlevs genom hela leverantörskedjan.

- **Övervaka prestanda**: Säkerställ att det finns en tillräckligt detaljerad övervakning av modellens prestanda. Följ upp och utvärdera för att se till att AI-tjänsten presterar på ett önskvärt sätt i enlighet med syftet. Det är viktigt för att kunna upptäcka och hantera avvikelser från det normala, exempelvis om modellen i vissa fall producerar resultat som inte går att styrka i det aktuella materialet som har behandlats.

- **Hantera säkerhetsbrister**: Upprätthåll och utvärdera säkerheten i tjänsten genom regelbundna säkerhetsuppdateringar, genomför sårbarhetsanalyser och penetrationstester för att identifiera och åtgärda potentiella säkerhetsbrister i systemet. Det innebär att verksamheten måste ha tekniska lösningar som bland annat övervakar AI-systemets åtkomstloggar, händelseloggar samt in- och utdata. Säkerställ att endast starkt autentiserade och behöriga användare får tillgång till informationen i tjänsten för att förhindra dataintrång och skydda personuppgifterna som behandlas.

- **Upprätta beredskap för incidenter**: Inrätta en beredskapsplan för att upptäcka och hantera eventuella dataintrång eller oegentligheter i realtid, inklusive sådana intrång som kan utgöra en personuppgiftsincident enligt artikel 4.12 i dataskyddsförordningen. Snabb och effektiv hantering kan minska den potentiella skadan och säkerställa att organisationen kan uppfylla sina skyldigheter enligt artiklarna 33 och 34 i dataskyddsförordningen gentemot tillsynsmyndigheten och registrerade.

- **Arbeta riskmedvetet**: Beakta standarder som vägleder i det systematiska arbetet med risker. ISO/IEC 42001 är en internationell standard som fokuserar på hanteringen av risker och säkerhet i samband med användningen av AI. Standarden syftar till att skapa ett ramverk för att säkerställa att AI-system utvecklas och används på ett sätt som är säkert, etiskt och i enlighet med gällande lagar och förordningar. Vid implementeringen av språkmodeller kan dessa typer av standarder med fördel beaktas för att skapa en struktur och systematik för förvaltningen.

- **Hantera förändringar**: Nya versioner av språkmodeller släpps regelbundet när leverantörerna hittar nya metoder för att förbättra prestandan. Dessa förbättringar kan inkludera ökad noggrannhet, snabbare bearbetning och bättre hantering av komplexa språkliga sammanhang. Dessutom kan uppdateringarna åtgärda svagheter som upptäckts i tidigare versioner. För att säkerställa att organisationen effektivt hanterar upptäckta brister i den valda tekniken är det viktigt att det finns en plan för hur modellen ska kunna bytas ut vid behov. Denna plan bör inkludera en utvärdering av modellerna för att kunna bedöma prestanda och säkerhet jämfört med den nuvarande modellen, men även testning och validering innan implementation för att säkerställa att den nya språkmodellen uppfyller samtliga krav som organisationen ställer på tjänsten.

Slutligen betonar IMY att en konsekvensbedömning alltid ska göras om en viss typ av behandling sannolikt leder till hög risk för registrerades rättigheter och friheter. Den förteckning som har tagits fram av IMY kompletterar dataskyddsförordningens bestämmelser över när en konsekvensbedömning behöver genomföras. För användning av tjänster likt den maskeringstjänst som Lidingö stad önskar ta i bruk anser IMY att det typiskt sett innebär:

- behandling av känsliga personuppgifter enligt artikel 9 eller uppgifter som är av mycket personlig karaktär
- behandling av personuppgifter i stor omfattning
- behandling av personuppgifter om personer som av något skäl befinner sig i ett underläge eller i beroendeställning och därför är sårbara
- användning av ny teknik eller nya organisatoriska lösningar.

Sammantaget finner IMY att en sådan personuppgiftsbehandling som sker i samband med användningen av en AI-tjänst likt den aktuella maskeringstjänsten typiskt sett innebär att minst två kriterier i IMY:s ovannämnda förteckning anses vara uppfyllda och att en konsekvensbedömning enligt artikel 35 i dataskyddsförordningen därmed bör genomföras.