DPIA – Känsliga personuppgifter i Intrics plattform

Version 1

Beslutad av:
Beslutsdatum och paragrafnummer:
Diarienummer: KS 2026/0196-1
Dokumentansvarig avdelning: Digitaliseringsenheten

VARBERGS KOMMUN

Innehållsförteckning

DPIA – Känsliga personuppgifter i Intrics plattform 1
Version 1 1
1. Övervägande skyldighet att genomföra en DPIA.....3
2. Resultat av tröskelanalys 4
3. Systematisk beskrivning av personuppgiftsbehandlingen.....5
3.1 Behandlingens art.....5
3.2 Behandlingens omfattning 9
3.3 Behandlingens sammanhang 11
3.4 Behandlingens ändamål 12
3.5 Nödvändiga resurser.....14
3.6 Funktionell beskrivning av behandlingen 14
3.7 Roller och ansvarsfördelning 25
4. Rättslig analys 26
4.1 Dataskyddsprinciperna och rättslig grund för behandlingen26
4.2 De registrerades rättigheter 36
4.3 Skyddsåtgärder för internationella överföringar 39
4.4 Behandling utförd av personuppgiftsbiträde. 39
4.5 Sammantagen rättslig bedömning 41
5. Riskhantering 42
5.1 Identifiering av riskerna.....42
5.2 Strukturell observation från riskanalysen 43
7. Synpunkter från berörda.....44
7.1 Rekommendationer från dataskyddsombudet 44
7.2 Synpunkter från de registrerade 44
7.3 Synpunkter från övriga intressenter.....45
8. Sammantagen bedömning, förhandsvillkor 45
Förhandsvillkor och tekniska spärrar för driftsättning 46
9. Förankra bedömningen i organisationen.....47
10. Följ upp konsekvensbedömningen kontinuerligt 48
Uppföljning av AI-administratörens funktion 48
Personoberoende och kontinuitet 48

1. Övervägande skyldighet att genomföra en DPIA

Tabell 1 nedan belyser ett antal kriterier från GDPR (artikel 35.3) för när en konsekvensbedömning (DPIA) behöver göras. De planerade tillämpningssituationerna gör det sannolikt att det kommer att röra sig om omfattande behandling av personuppgifter.

Behandlingen omfattar särskilda kategorier av personuppgifter enligt GDPR (Artikel 9.1). Personuppgifterna kan vara av personlig karaktär.

Behandlingen avser uppgifter om personer som befinner sig i ett underläge eller beroendeställning och som därför är sårbara.

Behandlingen innefattar ny teknik som förväntas introducera nya och innovativa arbetssätt inom organisationen.

Kriterier	Ja	Nej	Kommentar
35.3 (a) Behandlingen innebär systematisk och omfattande bedömning av individers personliga aspekter som grundar sig på automatisk behandling, inbegripet profilering, och på vilken beslut grundar sig som har rättsliga följder för, eller på liknande sätt i betydande grad påverkar, individer.	☐	☒	
35.3 (b) Behandlingen innebär behandling i stor omfattning av särskilda kategorier av uppgifter, som avses i artikel 9.1, eller av personuppgifter som rör fällande domar i brottmål och lagöverträdelser som innefattar brott, som avses i artikel 10.	☒	☐	
35.3 (c) Behandlingen innebär systematisk övervakning av en allmän plats i stor omfattning.	☐	☒	
IMY (1) Behandlingen omfattar utvärdering eller poängsättning av människor.	☐	☒	
IMY (2) Behandlingen syftar till att fatta automatiserade beslut som har rättsliga följder eller liknande betydande följder för den registrerade.	☐	☒	
IMY (3) Behandlingen innebär systematisk övervakning av människor.	☐	☒	
IMY (4) Behandlingen omfattar känsliga personuppgifter enligt artikel 9 eller uppgifter som är av mycket personlig karaktär.	☒	☐	
IMY (5) Behandlingen rör personuppgifter i stor omfattning.	☒	☐	
IMY (6) Behandlingen kombinerar personuppgifter från två eller flera behandlingar på ett sätt som avviker från vad de registrerade rimligen kunnat förvänta sig.	☐	☒	
IMY (7) Behandlingen avser uppgifter om personer som av något skäl befinner sig i ett underläge eller i beroendeställning och därför är sårbara	☒	☐	
IMY (8) Behandlingen inbegriper ny teknik eller nya organisatoriska lösningar.	☒	☐	
IMY (9) Behandlingen syftar till att hindra registrerade från att få tillgång till en tjänst eller ingå ett avtal.	☐	☒	
Övriga risker			
Behandlingen innebär att uppgifter överförs till tredjeland (utanför EU/EES)		Nej	
Behandlingen innebär risk för att uppgifter överförs till tredjeland (utanför EU/EES)		Nej	

Tabell 1: Behandlingen med utgångspunkt från ett antal kriterier från GDPR (artikel 35.3).

2. Resultat av tröskelanalys

Tröskelanalysen visar att den planerade behandlingen sannolikt leder till hög risk för personers rättigheter och friheter enligt GDPR (Artikel 35.1). Förutsättningarna för den tilltänkta behandlingen innebär att kraven för konsekvensbedömning därmed är uppfyllda. En DPIA skall därför genomföras före behandlingen inleds.

Kommunen bedömer att DPIA:n skall genomföras som en gemensam DPIA på kommunövergripande nivå, då det är förenligt med vad som är tillåtet enligt artikel 35.1, andra meningen.

DPIA:ns scope omfattar inte behandling av sekretessbelagda uppgifter. Avgränsningarna redovisas i avsnitt 3.1. Utredningsbehovet beskrivs i bilaga 5, ”Sekretessfrågan i Intrics AI-plattform. Utredningsbehov och fortsatt arbete.

3. Systematisk beskrivning av personuppgiftsbehandlingen

3.1 Behandlingens art

Allmän beskrivning och bakgrund

Varbergs kommun, fortsättningsvis kallad ”kommunen” står inför ett flertal utmaningar och har ett antal behov som i olika utsträckning kan hanteras och tillgodoses genom genomtänkta tillämpningar av Artificiell intelligens (AI). En av utmaningarna är till exempel att ta hand om ett ökande behov av vård och omsorg, samtidigt som arbetskraften minskar. Kommunen behöver finna sätt att utföra mer arbete med mindre resurser. Därför finns ett behov av att effektivisera och anpassa kommunens tjänster och processer i önskad riktning. AI bedöms vara en viktig del i denna omställning. Kommunen har kommit en bit i sin AI-resa och medarbetarna har bland annat uppmuntrats att testa att arbeta med AI i begränsad omfattning och under kontrollerade former.

Kommunfullmäktige fastslår i kommunens mål att Varbergs kommun skall sträva mot att vara en effektiv och innovativ organisation som präglas av samarbete och stark förändringsvilja och -förmåga.[1] Ett prioriterat mål är att kommunen skall vara en effektiv och innovativ organisation som utvecklar verksamheten utifrån invånarnas perspektiv. Bland annat skall kommunens kommunikation samordnas, samlas och digitaliseras för ökad kvalitet, effektivitet och effekt.

Kommunens digitaliseringsstrategi förtydligar att varje verksamhet har ett ständigt ansvar att arbeta för att förenkla, förnya och förbättra sitt uppdrag, både genom att utveckla befintliga arbetssätt och genom att tänka på nya och innovativa sätt.[2] Digitaliseringsenheten har bedömt att AI-teknik i detta sammanhang kommer att tillföra ett betydande mervärde för organisationen.

Kommunens strategiska mål för AI är att på kort sikt öka användningen av AI hos medarbetarna i Varbergs kommun, samt höja medarbetarnas kunskaper i ämnet.[3]

AI-strategin och digitaliseringsstrategin är två exempel på hur kommunens uppdrag och mål konkretiseras. Slutsatsen är att AI-teknik utgör ett allmänt intresse, givet att behandlingen som görs är proportionerlig och nödvändig.

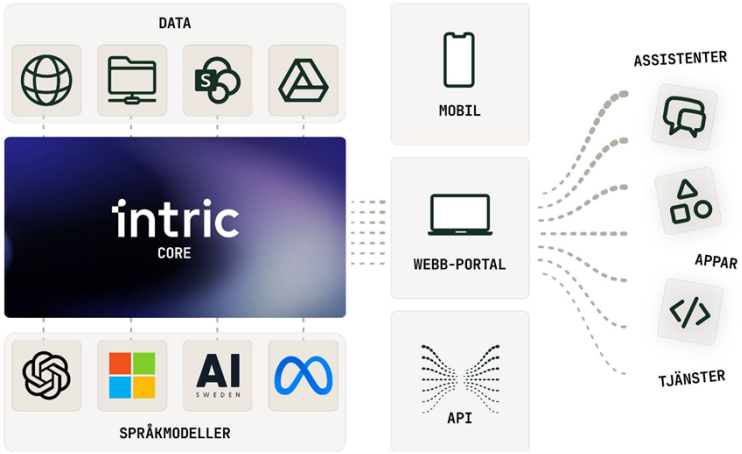
Företaget Intric AB, fortsättningsvis kallad Intric, tillhandahåller en omfattande AI-plattform, fortsättningsvis kallad AI-plattform, som är avsedd att skräddarsys

[1] Mål och inriktning 2024-2027 Varbergs kommun (KS 2022/0563)
[2] Digitaliseringsstrategi (2025/0387-1)
[3] Strategi för AI i Varbergs kommun (KS 2025/0412-1)

efter varje kunds behov (Figur 1). AI-plattformens målgrupp är främst offentlig sektor. Varbergs kommun har under en testperiod använt en avgränsad del av AI-plattformen – en AI-assistent. Syftet var att utvärdera tekniken utifrån de förutsättningar och behov som råder i Varbergs kommun.

Sammanlagt bjöds 416 medarbetare in att delta i testet. Av dessa skapade 234 ett användarkonto och deltog i testet. 114 medarbetare genomgick utbildning för rollen ”Creator”. Inom denna grupp valde 92 % att aktivera sitt konto. Det indikerar att utbildning och tydligt ansvar bidrar till att skapa engagemang. Testperioden löpte ut i 2026-04-27 varpå deltagarnas synpunkter samlades in och AI-assistenten utvärderades. En DPIA avseende det genomförda testet av AI-assistenten har genomförts, dock med avgränsning specifikt till AI-assistenten i Intrics AI-plattform, och behandling av text utan förekomst av känsliga personuppgifter.[4]

Medarbetare som deltog i testet har framfört önskemål om att nyttja AI-plattformens samtliga funktioner i sina respektive verksamheter. Detta inkluderar transkribering av tal, samt möjlighet att behandla känsliga personuppgifter. De verksamheter som kommit längst och är drivande inom AI-tillämpningar har signalerat att den ovan beskrivna omställningen hämmas av att inte kunna tillämpa AI även på känsliga personuppgifter.



Figur 1: Intric, en översikt.

Avgränsningar och antaganden

Motivering till avgränsningen mot sekretess

Frågan om hur uppgifter av sekretess enligt offentlighets- och sekretesslagen (2009:400) får behandlas i en AI-plattform med externt personuppgiftsbiträde aktualiserar ett i flera avseenden oklart rättsläge. Det berör tolkningen av 10 kap. 2 a § OSL om sekretessgenombrott vid teknisk bearbetning, frågan om huruvida AI-inferens utgör ”endast teknisk bearbetning” i lagens mening, samt en rad

[4] DPIA AI-assistent med Intrics AI-plattform (KS 2025/0526)

sektorsspecifika regelverk såsom socialtjänstens registerförfattningar (SoLPUL och SoLPUF), patientdatalagen och skolsekretessens uppdelning enligt 23 kap. OSL.

En DPIA enligt GDPR art. 35 är ett instrument för att bedöma och hantera dataskyddsrisker, under förutsättning att behandlingen har laglig grund. Den är inte avsedd att vara ett verktyg för samlad rättslig utredning av angränsande rättsområden. Därav följer att försök att inom ramen för denna DPIA försöka avgöra sekretessfrågan skulle riskera antingen ett bristfälligt underlag, eller en överskattning av DPIA-processens räckvidd. Båda riskerna torde vara till nackdel för såväl de registrerade som för kommunens efterlevnadsarbete.

Sålunda har kommunen valt att avgränsa denna DPIA till behandling av känsliga personuppgifter som inte omfattas av sekretess enligt OSL. Sekretessfrågan hanteras separat enligt bilaga 5, och kräver särskild juridisk bedömning i varje enskilt användarfall innan AI-plattformen får tas i drift för sådana uppgifter.

Avgränsningens utformning är avsiktligt konstruerad för att vara skyddande snarare än underlåten. Det vill säga, det skall inte vara möjligt att felaktigt tolka avgränsningen som ett godkännande för behandling av sekretessbelagda uppgifter genom passivitet. Vidare måste konstruktionen tillämpas operativt för att avsedd verkan skall uppnås. Detta sker genom de förhandsvillkor och tekniska spärrar som anges i kapitel 8.

Avgränsningar

1. Denna DPIA avser att fastställa en gemensam ram för all behandling av känsliga personuppgifter i AI-plattformen i hela kommunen, inklusive särskilda kategorier av personuppgifter enligt GDPR (Artikel 9.1).
2. Det åligger varje personuppgiftsansvarig nämnd eller bolag som inleder en behandling, vilken omfattar känsliga personuppgifter enligt denna DPIA, att registrera behandlingen i sitt behandlingsregister. Därjämte skall den personuppgiftsansvarige bedöma huruvida den planerade behandlingen väsentligt avviker från denna DPIA. Om så är fallet skall en kompletterande DPIA genomföras.
3. Behandling av sekretessbelagda uppgifter täcks inte av denna DPIA. Sådan behandling är ett angränsande rättsområde som bör analyseras genom en eller flera separata juridiska bedömningar. Se bilaga 5.
4. På grund av avgränsningen i punkt 3 ovan blir personuppgiftsansvarigas behov av DPIA gällande behandling av sekretessbelagda uppgifter inte tillgodosett.
5. Användning av AI-plattformen för uppgifter som omfattas av sekretess enligt OSL får inte påbörjas. Säkerhetsklassningen i AI-plattformens Security Classification-funktion skall därför konfigureras så att

verksamheter med sådana uppgifter inte kan aktivera plattformen för denna typ av uppgifter innan ny DPIA och separat juridisk bedömning genomförts av varje personuppgiftsansvarige som önskar behandla sekretessuppgifter i AI-plattformen.

Antaganden

1. Kommunen avser att använda samtliga funktioner som vid tidpunkten för denna DPIA finns tillgängliga i AI-plattformen.
2. För känsliga personuppgifter skall kommunen använda en språkmodell vars beräkning sker på GPU-kapacitet hos Intrics underbiträde AI Iron AB (559490-8054), med hosting i Sverige.
3. För transkribering av känsliga personuppgifter skall kommunen använda transkriberingsmodellen KB-Whisper, vilken hostas av Intrics underbiträde Berget AI AB (559504-7522), med hosting i Sverige.

Kategorier av personuppgifter

För att AI-plattformen skall fungera behandlas följande personuppgifter tillhörande användarna:

- förnamn
- efternamn
- ip-adress
- sessions-id och cookies

Personuppgifterna inhämtas från AD-systemet och användarens webbläsare. Användaren kan själv välja att lämna ytterligare personuppgifter i interaktionen med webbportalen. Dessa kan bestå av allmänna personuppgifter eller särskilda kategorier av personuppgifter:

Allmänna personuppgifter

- förnamn
- efternamn
- personnummer
- samordningsnummer
- bankkontonummer
- användar-ID
- e-postadresser
- organisationstillhörighet
- tekniska data såsom IP-adress, aktivitetsloggar
- innehåll i promptar, bilagor
- innehåll i kunskapssamlingar som användaren samlar i AI-plattformen

Särskilda kategorier av personuppgifter (Artikel 9.1)

- uppgifter som avslöjar etniskt ursprung
- uppgifter som avslöjar politiska åsikter
- uppgifter som avslöjar religiös eller filosofisk övertygelse

- uppgifter om medlemskap i fackförening
- uppgifter om hälsa
- uppgifter om sexualliv och sexuell läggning

Följande kategorier av särskilda personuppgifter behandlas inte:

- uppgifter om ras
- biometriska uppgifter
- genetiska uppgifter

Kategorier av registrerade

Följande kategorier av registrerade omfattas av behandlingen:

- anställda som använder AI-plattformen
- förtroendevalda som använder AI-plattformen

Följande kategorier av registrerade omfattas av behandlingen i den mån personuppgifter förekommer i det material som behandlas i AI-plattformen:

- invånare
- elever
- vårdnadshavare
- sökande till anställningar och praktikplatser
- besökare
- externa parter i kommunens ärenden
- personer som förekommer i beslutsunderlag, protokoll, mail eller interna dokument.

3.2 Behandlingens omfattning

Behandlingens volym

Eftersom syftet med AI-plattformen är att effektivisera, förväntas införandet på sikt innebära att AI ersätter nuvarande arbetssätt och verktyg. AI-plattformen kan komma att användas av samtliga kommunens drygt 5000 anställda som har dator som ett dagligt arbetsverktyg. Det skulle betyda verksamheternas behandling av personuppgifter i praktiken förflyttas från ett verktyg till ett annat.

En osäkerhetsfaktor för att beräkna volym är beteendet hos användarna. Detta då det inte finns något som hindrar att användarna laddar upp material som innehåller större volymer med personuppgifter. Ytterligare en osäkerhetsfaktor AI-plattformen funktionalitet och användbarhet i hög grad påverkar behandlingens volym. Innehållet i enskilda användares uppladdade material skulle kunna få stor påverkan på den sammanlagda behandlingsvolymen. Det går

inte att utesluta att användare laddar upp stora mängder personuppgifter i AI-assistenten.

Slutsatsen är att det på sikt kommer innebära en omfattande behandling av personuppgifter, som ökar i takt med utfasningen av befintliga arbetssätt och verktyg. Möjligheten att behandla stora datamängder skulle kunna medföra att behandlingens omfattning totalt sett ökar.

Behandlingens varaktighet

Personuppgifter knutna till användarkonton raderas när kontot avslutas. Tekniska loggar raderas efter fem år om inte annat angivits av kommunen. Uppladdade dokument och chattloggar gallras i enlighet kommunens konfigurerade gallringsregler. Specifikt för känsliga personuppgifter gäller att varje personuppgiftsansvarige skall konfigurera gallringreglerna med utgångspunkt från den aktuella behandlingen samt den egna förvaltningens eller bolagets dokumenthanteringsplan.

Behandlingens geografiska omfattning

För behandling av känsliga personuppgifter har kommunen konfigurerat plattformen i enlighet med Tabell 2, nedan, så att all bearbetning sker inom Sverige eller inom EU. Tredjelandsöverföringar är blockerade för känsliga personuppgifter. Detta sker i Intrics säkerhetsklassificeringsfunktion (Security Classification) vilken säkerställer att modeller och verktyg som driftas utanför EU är inaktiverade i de sammanhang där verksamheterna tillåts behandla känsliga personuppgifter.

MCP/OAuth-verktyg är hostade hos GleSys AB i Sverige. Dock kan externa servrar som verktygen anropar geografiskt ligga var som helst. Detta på grund av att dessa är tredjepartsservrar utanför Intrics kontroll.

Komponent	Underleverantör	Hosting/Lokalisering
Intric-plattformen (kärna)	GleSys AB	Sverige
Språkmodell (LLM) för känsliga personuppgifter	AI IRON AB (Airon)	Sverige
Kunskapssamlingar (Knowledge)	AI IRON AB (Airon)	Sverige
Avidentifiering (Redaction)	AI IRON AB (Airon)	Sverige
Transkribering	Berget AI AB	Sverige
MCP / Oauth-verktyg	GleSys AB	Sverige
Websök (om aktiverad)	LinkUp	Frankrike (EU)

E-postutskick (Plattform AI)	Scaleway	Frankrike (EU)
Tredjelandsöverföringar	**Blockerade för känsliga personuppgifter**	Får ej förekomma

Tabell 2: Sammanställning över komponenter, underleverantörer och lokalisering.

3.3 Behandlingens sammanhang

Behandlingen sker inom ramen för kommunens offentliga verksamhet. AI-assistenten är avsedd att utgöra ett internt arbetsredskap för kommunens medarbetare.

Medarbetarna har möjlighet att skriva in eller ladda upp olika former av material som AI-Assistenten hjälper medarbetarna att behandla. AI-assistentens utdata granskas alltid manuellt av medarbetaren innan det används som till exempel beslutsunderlag eller delges antingen internt eller externt.

AI-assistentens behandling kommer att innebära ny behandling av befintliga personuppgifter. Inga nya kategorier av personuppgifter samlas från de registrerade för att användas i AI-assistenten. Materialet förekommer redan i kommunen i verksamhetssystem, e-post och interna dokument. AI-assistenten är ett nytt tekniskt verktyg för att stödja medarbetarna i arbetet.

Den ovan beskrivna behandlingen i AI-assistenten sker som en del av kommunens omställning och i syfte att förenkla och effektivisera arbetsuppgifter.

IT-avdelningen har presenterat statistik som visar att medarbetarna under en 90-dagarsperiod 2026 använt minst 104 olika AI-tjänster.[5] Statistiken bekräftar att AI redan används i mycket hög utsträckning på förvaltnings- och bolagsnivå. Det påvisar att medarbetare i hög omfattning använder tjänster som de valt ut på egen hand, och att privata konton används. Användandet är en indikator på att medarbetarna är engagerade i frågan och har en vilja att testa ny teknik. Detta är värdefullt för kommunen, men samtidigt också problematiskt ur informationssäkerhets- och dataskyddsperspektiven. Bland annat eftersom det innebär att kommunen förlorar kontrollen över sina informationstillgångar, vilka även kan innehålla personuppgifter.

[5] bilaga 4 - rapport ai-användande.xlsx

Införandet av AI-assistentens samtliga funktioner, med möjlighet att även behandla känsliga personuppgifter, innebär att kommunen fattar ett formellt beslut att införa tekniken och även hänvisar till en säker lösning, med samma funktionalitet som den skugg-it som vuxit fram.

AI-assistenten kommer på sikt att göras tillgänglig för samtliga medarbetare som fullföljt en AI-utbildning, har tillgång till en arbetsdator, samt har tilldelats ett användar-id i organisationens AD. Initialt begränsas dock användningen genom rollbaserad behörighetsstyrning (RBAC) till de verksamheter som fullföljt nödvändigt förberedande arbete såsom utbildning av användarna, utredning om en kompletterande DPIA behöver genomföras, identifiering av de behandlingar som är specifika för den egna verksamheten, samt registrering av behandlingen i sina respektive behandlingsregister.

Behandling av personuppgifter kommer att vara aktuell i ett sammanhang där medarbetare skapar och förädlar text, i vissa fall sammanfattar samtal, eller har behov att konsultera styrdokument, rutiner och annat textmaterial.

De registrerades relation till kommunen såväl som medarbetarnas anställningsförhållande med kommunen kan definieras som varierande grad av beroendeställning, eller i vart fall en svagare position gentemot kommunen. Det är därför troligt att de registrerade har en hög förväntan på olika aspekter gällande behandlingens korrekthet, säkerhet och att det inte fattas automatiserade beslut. Även om AI snabbt fått en bred spridning i samhället så är det troligt att registrerade i många fall inte kan förvänta sig eller förutse att deras uppgifter behandlas av en språkmodell. Därför är transparens och information till de registrerade särskilt viktigt.

3.4 Behandlingens ändamål

Det övergripande ändamålet med behandlingen är att stödja kommunens medarbetare i deras arbete med att utföra arbetsuppgifter av allmänt intresse, samt att bidraga till kommunens digitalisering och omställning i enlighet med kommunens digitaliseringsstrategi och AI-strategi.

Eftersom kommunen väljer att använda AI-assistentens samtliga funktioner, utgår behandlingens specifika ändamål att stödja medarbetarna från denna funktionalitet att:

1. sammanfatta, analysera och generera underlag utifrån användarnas och verksamheternas input.
2. söka information i kommunens interna dokument som finns uppladdade i AI-assistenten.

3. transkribera ljudfiler från sammanhang där det bedömts lämpligt samt bearbeta och sammanfatta resultatet.
4. avidentifiera dokument inför vidare behandling.
5. utforma utkast till interna och externa dokument såsom brev, beslutsförslag, email vilka därefter granskas manuellt och färdigställs av handläggaren.
6. söka information på internet.

Generella arbetsuppgifter som AI-assistenten förväntas tillgodose genom funktionaliteten:

- skrivstöd vid textproduktion
- förslag till formuleringar vid textproduktion
- feedback på befintlig text
- förbättringsförslag på befintlig text
- språkstöd vid skapande av ny text
- översättning vid skapande av ny text
- hjälpa medarbetare att få kunskap om gällande arbetsrutiner
- fakta- och datainsamling
- hjälp med att förbereda möten
- stöd vid projektplanering vid uppstart av nya projekt
- stöd vid projektplanering vid befintliga projekt
- utbildning och kompetensutveckling från befintligt material
- utbildning och kompetensutveckling genom att fråga AI-assistenten
- hjälp med dataanalys för beslutsfattande
- transkribera, sammanfatta och dokumentera möten
- stöd vid sekretessmarkering av dokument

3.4.1 Vilka behov som tillgodoses

De behov som tillgodoses är:

- frigörande av tid genom effektivare hantering av administrativa arbetsuppgifter
- högre kvalitet i underlag genom bättre överblick i omfattande material
- förbättrad service gentemot kommunens invånare genom snabbare handläggande

3.4.2 Uteblivna mervärden om behandlingen inte görs

Majoriteten av kommunens förvaltningar har en tung administrativ börda. Utan möjlighet att genomföra behandlingen går kommunen miste om effektiviseringsvinster och kvalitetsförbättringar som skulle realiseras hos de verksamheter som annars skulle genomföra behandlingen. Indirekt skulle

kommunens invånare gå miste om potentiellt bättre service. Det har även gjorts gällande att organisationer som inte anammar AI-teknik upplevs som mindre attraktiva arbetsgivare än de organisationer som ligger i framkant och använder AI. En konsekvens av detta skulle kunna vara att kommunen på sikt får svårare att rekrytera medarbetare med önskvärd kompetens.

3.5 Nödvändiga resurser

För att kunna behandla känsliga personuppgifter i AI-assistenten krävs:

En dedikerad molninstans hos GleSys AB i Sverige.

Behandlingen förutsätter att användaren har ett användar-id samt dator eller mobil enhet för att ansluta till AI-assistenten.

Anslutning till kommunens identitetshantering - Active directory/Entra ID för Single Sign On (SSO) och (MFA).

Resurser för att säkerställa fullföljandet av riskreducerande åtgärder:

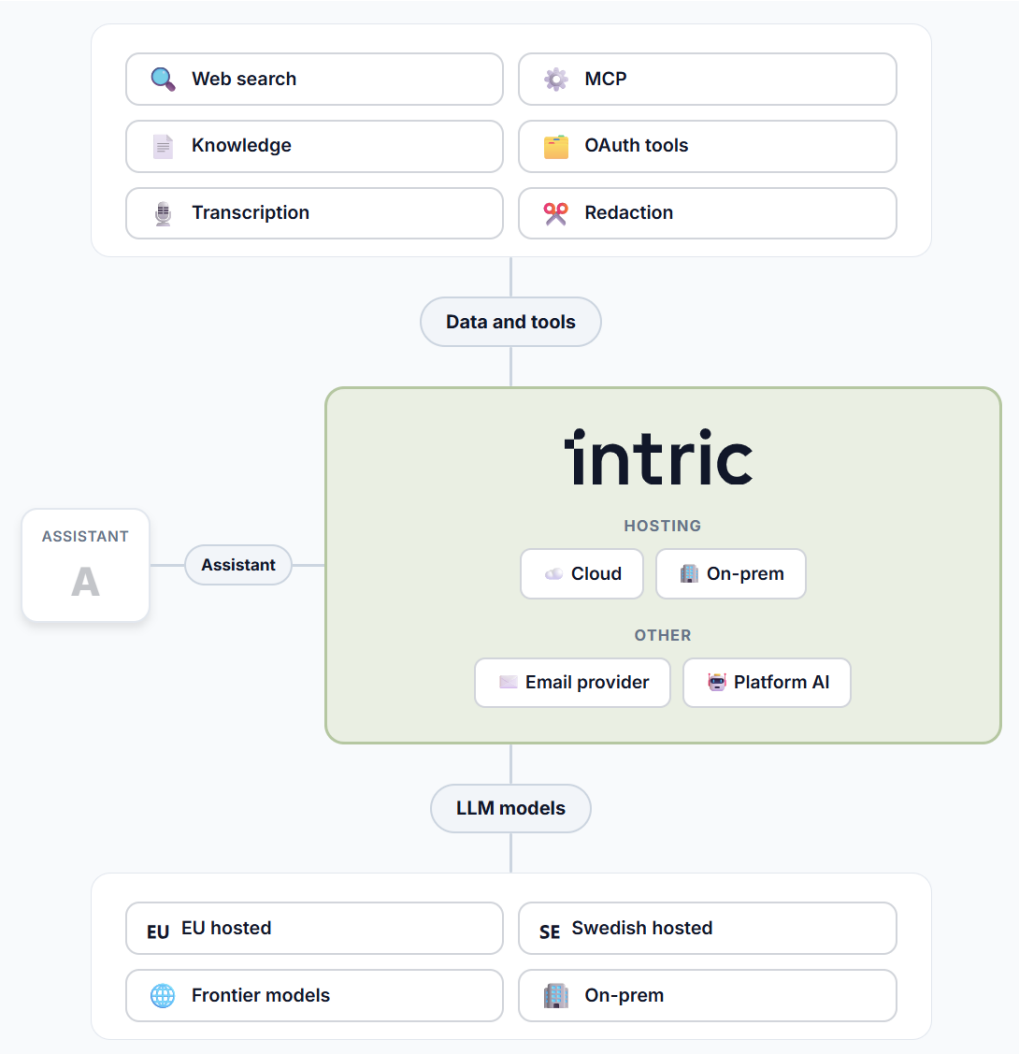
1. utpekad systemägare
2. systemförvaltare
3. huvudansvarig på varje förvaltning/bolag som stöd till systemförvaltaren
4. AI-administratör
5. dataskyddssamordnare på varje förvaltning/bolag
6. informationssäkerhetssamordnare på varje förvaltning/bolag
7. obligatorisk utbildning inom AI-användande, dataskydd och informationssäkerhet för användare som behandlar personuppgifter
8. riktlinjer, rutiner och anvisningar enligt kommunens AI-strategi, samt kompletterande rutiner på förvaltningsnivå
9. tekniska skyddsåtgärder, främst rollbaserad behörighet, säkerhetsklassning, loggning och automatisk gallring
10. resurs på kommunstyrelsens förvaltning som kontrollerar efterlevnad utifrån GDPR inklusive skyddsåtgärder och utbildningar
11. resursen i punkt 10 ovan skall ha fastställt mandat och uppdrag att kontrollera att det finns laglig grund för behandlingen på varje förvaltning/bolag innan behandlingen påbörjas

3.6 Funktionell beskrivning av behandlingen

Beskrivning Intrics AI-plattform

Intric är en AI-plattform som är specifikt utvecklad för offentlig sektor och företag med höga krav på säkerhet och personlig integritet. Intric fungerar som en knutpunkt mellan de personer som använder det, den data de arbetar med och

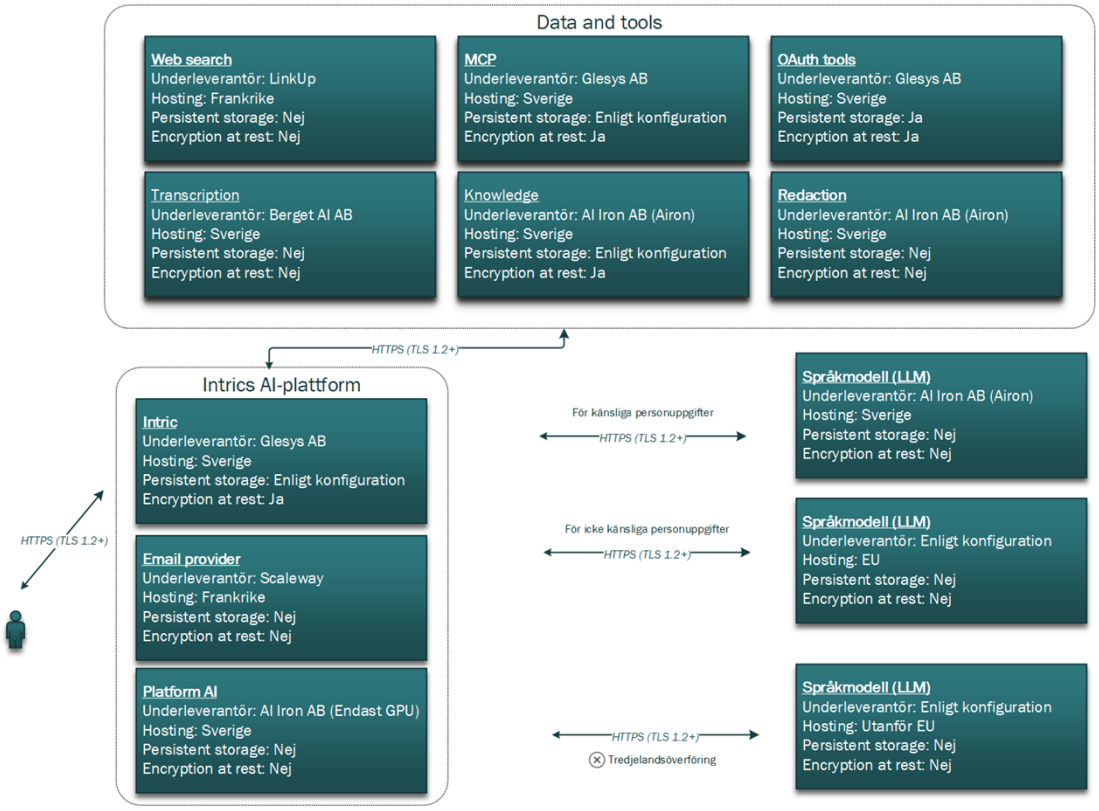
de AI-modeller som driver svaren. Figur 2, nedan visar hur dessa tre komponenter kopplas samman genom Intric och blir en samlad AI-assistent för användaren.



Figur 2: En överblick över Intrics AI-plattform och dess komponenter.

Dataflöde

Behandlingens dataflöde illustreras i Figur 3 nedan. Tekniskt stöds det konfigurerade dataflödet av plattformens funktion ”Security Classification”. Genom att ge ”spaces”, modeller och verktyg en anpassad säkerhetsklass för känsliga personuppgifter, kan den utpekade ansvarige administratören säkerställa att de assistenter som är avsedda för känsliga personuppgifter endast kan användas med komponenter som är godkända för den säkerhetsklassen.



Figur 3: AI-assistentens dataflöde.

Intric-plattformen och dess funktioner

Intric-plattformen fungerar som en kopplingspunkt mellan användare, organisationens data och de verktyg som organisationen väljer att aktivera. Den hanterar hämtning av information och anrop för att starta de verktyg och AI-modeller som organisationen har tillåtit.

Cloud Hosting

Kommunen har valt alternativet *cloud hosting*. Alternativet innebär att applikationen och kommunens information behandlas på en infrastruktur som drivs för Intric på servrar hos en svensk molnleverantör, GleSys AB. Servrarna är geografiskt placerade i Sverige. Den information som bearbetas på plattformen lagras i enlighet med de regler för lagring kommunen tillämpar.

Kryptering ”In transit” med TLS 1.2+ (HTTPS). Kryptering ”at rest” tillämpas. Krypteringsnycklar förvaltas av Intric med krypteringsalgoritm AES med 256-bitars kryptering.

Email provider

Email-provider som ingår i AI-plattformen är email-funktion som tillhandahålls av underleverantören Scaleway. Scaleway är ett franskt företag med servrar geografiskt placerade i Frankrike. Funktionen sänder email med systemrelaterat innehåll såsom notifieringar, inbjudningar eller statusuppdateringar gällande användande. Funktionen hanterar således inte känsliga personuppgifter.

Personuppgifter som förekommer i detta sammanhang lagras hos underleverantören endast så länge som är nödvändigt för att fullfölja det avtalade uppdraget, och raderas därefter. Datan är krypterad vid överföring (TLS 1.2+) mellan Intric-plattformen och Scaleway.

Platform AI

AI-plattformen täcker Intric-hanterade assistenter. Dessa använder en grundmodell och kan användas utan att välja en separat leverantör. Dessa assistenter är föremål för samma dataflödes- och kvarhållningsprinciper som övriga assistenter

Data and tools

Data och anslutna verktyg förser assistentlagret med information och stöd i form av websökningar, kunskapsunderlag, integrationer, transkription samt en funktion för bortredigering. Verktygen och informationen kombineras i Intric innan promptar och kontext skickas till utvalda modeller.

Web search

Websökningsverktyget möjliggör för AI-assistenter att hämta information från websökningar. Funktionen är deaktiverad för känsliga personuppgifter genom AI-plattformens säkerhetsklassning. Konkret innebär det att websökfunktionen inte är tillgänglig i de ”spaces” som är används för känsliga personuppgifter.

Underleverantören för denna funktion är LinkUp, ett franskt företag, vars servrar är geografiskt placerade i Frankrike. I de situationer där funktionen är tillgänglig, det vill säga för icke känsliga personuppgifter, är det enbart den AI-genererade sökfrågan som skickas till LinkUp, inte användarens prompt, chatthistorik eller bifogade filer. LinkUp tillämpar nolldatalagring (zero data retention), vilket betyder att data raderas omedelbart efter LinkUp levererat sökresultatet till Intric.

TLS kryptering tillämpas vid överföring mellan webbrowsern och plattformen, språkmodellen och LinkUp. Eftersom ingen information kvarhålls hos sub-processorn efter bearbetning är det inte relevant med ett separat krypteringslager *at-rest* för trafiken som härrör från sök-trafiken.

Knowledge

Kunskapsverktyget lagrar och indexerar dokument som laddas upp. Detta är nödvändigt för att assistenterna skall kunna hämta relevanta avsnitt av

informationen vid förfrågan. Bearbetningen innefattar Intrics lagring i Sverige (GleSys AB) samt den embedding-modell som verktyget konfigurerats till att använda.

För känsliga personuppgifter är embedding-modellen en svensk leverantör. Endera Berget AI AB (KB-Whispers tillhörande embedding-modell) eller AI Iron AB. De båda underbiträdena har servrar geografiskt placerade i Sverige. Vid bearbetningen sänds endast textfragment (”textchunks”) från uppladdade dokument till underleverantören. Ingen användaridentitet sänds med. Textfragmenten används därefter för att generera sökvektorer. Nolldatalagring (zero data retention) tillämpas hos underleverantören. All förekommande persistent lagring sker på Intrics servrar hos GleSys AB i Sverige. TLS-kryptering (TLS 1.2+) tillämpas vid överföring.

Transcription

Verktyget för transkribering producerar text av tal med möjlighet till sammanfattning. Ingen information lagras hos den leverantör som tillhandahåller AI-modellen (zero data retention policy).

Processen från ljuduppladdning till en färdig transkription och sammanfattning sker genom en SSL/TLS-krypterad interaktion mellan Intric-plattformen där datan hanteras och den LLM-leverantör kommunen har valt.

I Transkriberingsprocessen ingår följande steg:

1. Användaren laddar upp en ljudupptagning till Intric. Antingen genom Intrics transkriberingsverktyg eller i form av en inspelad ljudfil. I det senare fallet delas förutom ljudupptagningen filnamn och metadata. Uppladdning sker genom webbrowser. HTTPS används (TLS 1.2 eller högre) vid överföring mellan webbrowser och Intrics application API. Därmed är både ljud och eventuell bifogad metadata krypterad *in transit*. Uppgifter som är kopplade till användaren inloggning, (authenticaded Intric session) stannar på Intrics serverar under hela processen.

   At rest-kryptering tillämpas när datan lagras hos Intric (steg 2 och 5).

2. Intric tar emot, krypterar och lagrar filen i Intrics databas. Audio lagras i sitt originalformat. Metadatan lagras i JSON-format. Databasen som lagrar den krypterade ljudfilen tillhandahålls som infrastruktur av GleSys AB i Sverige. Den tekniska hanteringen, inklusive kryptering och dataminimering, utförs av Intric. Själva transkriberingsbearbetningen sker hos den valda transkriberingsleverantören (för känsliga personuppgifter: Berget AI AB). Databasen hanteras av en svensk underleverantör med servrar inom Sveriges gränser. Intric tar bort metadata innan audio sänds vidare externt för att processas. Det betyder

att ingen information om vem som laddade upp filen eller vilken organisation som den tillhör bifogas.

3. Data som innehåller ljudfil samt systeminstruktioner för transkribering och summering från Intric sänds till providern som har assistentens valda transkriberingsmodell. Det sker genom HTTPS (TLS 1.2+). Först generas en texttranskribering, därefter en sammanfattning.

4. Providern får inte information om användaren eller dennes organisations identitet. Dock med undantag av personuppgifter som användaren delar transkriberingsunderlaget. En förutsättning för att providern skall kunna utföra tjänsten är att audiofilen är tillgänglig för denne i läsbart, okrypterat format. TLS skyddar överföringen, men inte läsbarheten för mottagande part.

   Efter behandlingen sänder providern tillbaka resultatet i JSON-format. Det innehåller transkriberingen tillsammans med en sammanfattning. Intric tillämpar aktiv dataminimering. Underleverantören får bara tillgång till det material som är absolut nödvändigt för att utföra den avtalade tjänsten. Ingen data lagras hos underleverantören efter att leverantören levererat transkriberingen och sammanfattningen till Intric. Informationen används inte heller för att träna underleverantörens AI-modeller.

5. Transkriberingsmodellens resultat sänds till Intrics server. När överföringen har avslutats raderas ljudfil och det genererade resultatet omedelbart från providerns server. Överföringen av resultatet sker över HTTPS med kryptering *in transit* (TLS 1.2+)

   Intric tar emot, krypterar (*at rest*) och lagrar informationen i en databas.

6. Resultatet presenteras för användaren i dennes webbrowser. Överföringen sker via HTTPS med kryptering *in transit (TLS 1.2*). Konversationshistorik, transkriberingar, sammanfattningar, sparade ljudfiler och metadata krypteras och lagras i Intrics databas (*at rest*). I detta avslutande processteg förekommer användarens data endast i Intrics miljö.

Den LLM-leverantör som tillhandahåller transkriberingsmodellen för känsliga personuppgifter är Berget AI AB, vilken använder KB-Whisper-modellen, som utvecklats av Kungliga biblioteket, Berget AI AB använder servrar som är geografiskt placerade i Sverige. Berget AI AB tar emot ljudfiler för bearbetning,

men identifierande metadata om uppladdade användare och deras organisation tas bort av Intric innan filen sänds vidare. Nolldatalagring (zero data retention) tillämpas. Således lagras varken ljudfil eller bearbetad data hos Berget AI AB efter att resultatet levererats till Intric. Outputen, det vill säga transkribering samt i förekommande fall sammanfattning, lagras i Intrics databas hos GleSys AB i Sverige.

MCP

Model Context Protocol (MCP) används av AI-assistenten ansluta till externa verktyg.

Processen beskrivs i följande steg:

1. Användaren skriver ett meddelande till en AI-assistent som har ett eller flera MCP-verktyg. Datan sänds till Intrics server och innehåller användarens meddelande, chathistorik, samt eventuella filer som bifogats. Överföringen sker via HTTPS (TLS 1.2+) mellan användarens webbrowser och Intrics API.

2. Intric anropar den valda AI-assistentens språkmodell. I vissa fall behöver modellen använda ett verktyg för att fullfölja uppgiften. Bedömningen görs av modellen. När en sådan situation uppstår är det aktuellt att använda MCP. Modellen sänder en förfrågan till Intric att använda det nödvändiga verktyget.

   Ett praktiskt exempel är att modellen behöver söka efter statistik på en specifik hemsida för att fullfölja instruktionen från användaren. Överföringen mellan Intric och LLM sker över HTTPS (TLS 1.2+). Promptar och instruktioner lagras i klartext i LLM providerns ”trust zone” efter överföringen. Intric sänder inga uppgifter om användaren eller dennes organisation till tredje part. Personuppgifter som användaren delar i interaktionen med assistenten, och som är godkända enligt den konfiguration som gjorts, sänds dock vidare även till MCP-servern. Detta är nödvändigt för att MCP-serven skall fylla sin funktion. MCP-servrar kontrollerar sin egen lagring, Intric har därför ingen kontroll över till exempel MCP-serverns loggar. Språkmodellens leverantör sparar varken promptar eller svar.

3. Intric tar emot anropet från språkmodellen. Intric verifierar därefter att verktyget existerar och att förfrågan är tillåten. Därefter gör Intric anropet till MCP-servern i enlighet med språkmodellens förslag. All kommunikation till MCP-servern går via Intrics backend-server, aldrig direkt mellan språkmodellen och MCP-servern. Överföringen från Intric till MCP servern sker över HTTPS (TLS 1.2+).

4. MCP-servern tar emot förfrågan från Intric och ansluter till det verktyget i syfte att inhämta informationen som efterfrågas. Datakällan som verktygen hämtar från kan vara till exempel en databas, ett API, eller ett dokumentarkiv. MCP-servern hostas av Intric med servrar placerade hos Glesys AB. Underleverantören är ett svenskt företag med servrar placerade i Sverige.

   Överföringen mellan MCP-servern och datakällan använder kryptering in transit givet att datakällan har support för detta. Exempelvis TLS för de API:er som använder HTTPS, alternativt krypterad anslutning till databaser. I händelse av att den part som tillhandahåller datakällan saknar stöd för kryptering är överföringen mellan MCP och datakällan okrypterad.

5. MCP-servern bearbetar svaret från datakällan och returnerar svaret till Intrics server. Överföringen sker över HTTPS (TLS 1.2).

6. Intric sänder resultatet från frågan till språkmodellen som formulerar ett svar till användaren. Svaret baseras på både ursprungsfrågan och det svar som inkommit via MCP-servern. Överföringen mellan Intric och språkmodellen är krypterad över HTTPS (TLS 1.2+). Outputen från verktygen lagras i klartext (*at rest*) inom providerns trust zone.

7. Svaret presenteras för användaren. Data som lagras i Intric i detta skede är det genererade svaret och historiken från interaktionen med användaren. Överföringen mellan Intric och användarens webbrowser är krypterat över HTTPS (TLS 1.2+). Datan på Intrics server är krypterad (at rest).

För behandling av känsliga personuppgifter är användning av MCP-verktyg som ansluter till externa datakällor utanför kommunens kontroll (tredjepartstjänster) deaktiverad genom säkerhetsklassningen. Endast MCP-verktyg vars MCP-server hostas av Intric själv på servrar hos GleSys AB i Sverige får aktiveras i de spaces som är avsedda för känsliga personuppgifter. Innan ett MCP-verktyg aktiveras för känsliga personuppgifter ska AI-administratören verifiera att verktyget endast ansluter till MCP-servrar som driftas hos Intrics egendriftade servrar hos GleSys AB.

OAuth tools

Intric använder vissa verktyg som förutsätter att OAuth-integrerade tjänster används. Intric använder OAuth 2.3 för att koppla användare till

tredjepartstjänster. Ett exempel är att hämta dokument från SharePoint via API. I sådana situationer autentiserar sig varje användare direkt mot leverantören och godkänner de behörigheter. Med den här tekniken ser eller hanterar Intric aldrig användarens lösenord.

När en användare har godkänt anslutningen lagrar Intric åtkomsttoken och en refresh-token per användare och integration. Tokens krypteras med Fernet-kryptering (AES-128-CBC) innan de skrivs till databasen och dekrypteras enbart i minnet vid det ögonblick de behövs för ett API-anrop. Ingen token lagras i klartext och varje token är knuten till en enskild användare, det finns inga delade eller organisationsgemensamma tokens.

Processen innehåller följande steg:

1. Användaren interagerar med Intric via användarens webbrowser genom att skriva ett meddelande till en assistent som har en OAuth-integration. Anslutningen är krypterad *in transit* mellan browser och Intric genom HTTPS (TLS 1.2+).

2. Intric anropar den valda språkmodellen, som bedömer att ett verktyg bör användas. Språkmodellen returnerar en begäran via HTTPS (TLS 1.2+) om att använda den OAuth-autentiserade tjänsten.

3. Intric verifierar att assistenten har access till integrationen och att den aktuella användaren har en aktiv anslutning. Om åtkomst finns hämtar och dekrypterar Intric användarens åtkomsttoken. Om åtkomsttoken löpt ut använder Intric den senast sparade refresh-token för att hämta en ny åtkomsttoken, varvid den nya token som ersätter den gamla och krypteras och lagras. Lagringen sker i PostgreSQL med Fernetkryptering som bygger på AES-128-CBC, samt HMAC-SHA256. Hela processen sker utan att användaren behöver logga in igen.

4. När Intric har en giltig åtkomsttoken görs ett anrop till leverantörens API. Den giltiga åtkomsttoken inkluderas i anropets header för att autentisera begäran. I detta steg skickas åtkomsttoken tillsammans med åtgärd och de parametrar som språkmodellen specificerat, exempelvis filnamn eller en sökfråga. Språkmodellen kontaktar aldrig leverantörens API direkt, det vill säga all kommunikation sker via Intrics backendserver. Överföringen från Intric sker över HTTPS (TLS 1.2+).

5. Leverantörens API returnerar ett svar eller en bekräftelse till Intric. Data som skickas består av det begärda innehållet, till exempel dokumentets text eller metadata. Överföringen mellan leverantören och Intric sker över HTTPS (TLS 1.2+). Kryptering vid lagring (*at rest*) är möjlig och avgörs ytterst av de konfigurationsinställningar som kommunen väljer.

6. Intric skickar resultatet från verktyget och den kontext som behövs till assistentens valda språkmodell, så att modellen kan formulera ett svar som Intric vidarebefordrar till användaren. Överföringen mellan Intric och språkmodellen sker över HTTPS (TLS 1.2+).

7. Svaret visas i användarens webbrowser. Data som lagras på Intrics servar består av det genererade svaret tillsammans med metadata och historik över användarens interaktion med assistenten. Kryptering vid lagring är möjligt inom PostgreSQL. Omfattningen av historiken avgörs av assistentens gallringsinställningar. Överföringen till användarens webbrowser sker över HTTPS (TLS 1.2+).

För behandling av känsliga personuppgifter ska OAuth-integrationer endast aktiveras efter en särskild bedömning av AI-administratören. Detta då OAuth-anrop går till tredjepartens egna API:er såsom Microsoft Graph eller Google och datan därmed kan komma att behandlas i tredjepartsleverantörens infrastruktur, behöver respektive integration prövas separat med avseende på lokalisering, dataskydd och tystnadspliktsskydd. Inga Intric specifika underbiträden är inblandade i OAuth-anrop utöver den valda LLM-leverantören.

Redaction

Intric har en maskeringsfunktion som gör det möjligt att automatiskt upptäcka och maskera känslig information i uppladdade PDF-dokument. Syftet med funktionen är att hjälpa användaren att skydda personliga och konfidentiella uppgifter när användaren skall dela eller bearbeta dokument.

Intric använder en tvåstegsprocess för att identifiera och lokalisera känslig information:

1. I det första steget används AI-detektering. Assistentens valda kompletteringsmodell skannar varje sida individuellt och identifierar entiteter som matchar de kategorier du har valt (t.ex. namn, identifikationsnummer, finansiella uppgifter eller medicinsk information).

2. I det andra steget genomförs en koordinatmappning. När entiteterna har identifierats lokaliserar Intric deras exakta positioner i PDF:en genom att matcha den detekterade texten mot dokumentets layout. Detta bestämmer de exakta avgränsningsrutorna som används för maskering.

Följande detekteringskategorier är möjliga;

Personuppgifter:

- namn
- e-postadresser
- telefonnummer
- svenska personnummer
- personliga datum (t.ex. födelsedagar) och personliga platser (t.ex. hemadresser)

Företagsnamn:

- organisationsnamn
- svenska organisationsnummer
- organisationsrelaterade platser

Platser:

- gatuadresser
- postnummer
- städer
- länder och andra geografiska referenser

Finansiellt:

- kreditkortsnummer
- IBAN/bankkontonummer
- amerikanska socialförsäkringsnummer
- belopp
- fakturanummer
- momsnummer

Medicinskt:

- medicinsk information
- diagnoser
- behandlingar

Datum och tid:

- alla datum och tider i valfritt format

Anpassade kategorier:

- egna fritextkategorier

För behandling av känsliga personuppgifter använder Redaction-funktionen en kompletteringsmodell hos en av två svenska underleverantörer. Berget AI AB eller AI Iron AB. PDF-textens innehåll analyseras av modellen för att identifiera känslig information. Koordinatmappingen sker internt i Intric. Nolldatalagring (zero data retention) tillämpas hos underleverantören.

3.7 Roller och ansvarsfördelning

Roll	Innehavare
Personuppgiftsansvarig	Kommunstyrelsens förvaltning, Varbergs kommun, för kommunövergripande användning. Respektive nämnd eller bolag är personuppgiftsansvarig för den behandling som sker inom dess verksamhet.
Personuppgiftsbiträde	Intric AB (559308-3743)
Personuppgiftsunderbiträden (för känsliga personuppgifter)	GleSys AB (556647-9241), AI Iron AB (Airon) (559490-8054), Berget AI AB (559504-7522), Övriga underbiträden i PUB-avtalets Bilaga 2 är inte aktiverade för behandling av känsliga personuppgifter.
Dataskyddsombud	Karin Malmsten
GDPR-samordnare	Camilla Dahl, kommunstyrelsens förvaltning
Informationssäkerhetssamordnare	Camilla Dahl, kommunstyrelsens förvaltning
Avtalskontakt	Ingrid Halvorsen, digitaliseringschef, kommunstyrelsens förvaltning
Systemägare	Ingrid Halvorsen, digitaliseringschef, kommunstyrelsens förvaltning
Systemförvaltare	Daniel Leon, utvecklingsstrateg, kommunstyrelsens förvaltning
AI-administratör	Ny roll, ej utsedd
DPIA	Per Eriksson, dataskyddsstrateg, kommunstyrelsens förvaltning

DPIA:n har genomförts av dataskyddsstrateg i nära samverkan med utvecklingsstrateg digitaliseringsenheten, GDPR-samordnare, informationssäkerhetssamordnare. Dataskyddsombudet har konsulterats.

Underlag har inhämtats från Intric AB i form av utkast PUB-avtal, dokumentation av tekniska och organisatoriska säkerhetsåtgärder samt Statement of Applicability för Intrics ISO 27001-certifierade ledningssystem.

4. Rättslig analys

4.1 Dataskyddsprinciperna och rättslig grund för behandlingen

Laglighet korrekthet och öppenhet (artikel 5.1 a)

Artikel 5.1 a ger uttryck för tre principer. Tillsammans innebär de att personuppgifter skall behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade.

4.1.1 Laglighet

Behandling av personuppgifter är enligt artikel 6.1. e laglig endast om den är nödvändig för att utföra en uppgift av allmänt intresse, eller som ett led i den personuppgiftsansvariges myndighetsutövning. Det allmänna intresset eller myndighetsutövningen måste komma till uttryck i unionsrätten eller i nationell rätt (Art. 6.3). Enligt svensk rätt måste uppgifter av allmänt intresse som rättslig grund följa av lag eller annan författning (Lag 2018:218 med kompletterande bestämmelser till EU:s dataskyddsförordning, dataskyddslagen 2 kap 2 §).

Syftet med den aktuella behandlingen är dels att realisera kommunens omställning och effektivisering genom att införa AI som ett arbetsredskap, dels att bidra till kommunens digitalisering i enlighet med kommunens digitaliseringsstrategi och AI-strategi.

Slutsatsen är att rättsliga grunden för behandlingen är allmänt intresse (Art. 6.1.e).

4.1.2 Korrekthet

Principen om korrekthet innebär att all behandling av personuppgifter skall vara rättvis, skälig, rimlig och proportionerlig i förhållande till den registrerade. Korrekt behandling kräver att personuppgifterna är adekvata, relevanta och inte överflödiga i förhållande till ändamålet. Ej heller får behandlingen ske på ett sätt som är missgynnande, diskriminerande, oväntat eller vilseledande ur den registrerades perspektiv.

Ett problem med AI-teknik är att AI-modeller kan vara partiska. Det kan resultera i att outputen som AI skapar kan vara partisk eller diskriminerande.

Detta är relaterat till hur modellen tränats och vilken data som används. Bias kan vara uppenbar men den kan också vara svår att upptäcka. Detta bör ses som en inbyggd risk i AI-teknik. Således bör kommunen förutsätta att problemet med bias kan förekomma i olika sammanhang även i Intrics AI-plattform.

Riskanalysen uppmärksammar risken för att diskriminering uppstår i AI-plattformen genom att bias kan förekomma i de algoritmer som används.[6] I ett tänkbart scenario gällande AI-plattformen, skulle det kunna leda till att personuppgifter inte behandlas på ett rättvist, skäligt, rimligt och proportionerligt sätt i förhållande till den registrerade, vilket strider mot principen om korrekthet.

Kommunen bedömer att det i detta sammanhang är nödvändigt att välja modeller vars egenskaper är möjliga att utvärdera och följa upp. Samt att genomföra manuell granskning av all utdata från AI-plattformen. Granskningsprocessen bygger på att användaren omedelbart granskar det material som AI-plattformen genererar. Det i sin tur har inbyggda risker kopplat till mänskliga fel och misstag. Som exempel är det tänkbart att bristande utbildning, hos granskaren leder till att steget hoppas över eller inte genomförs grundligt. En konsekvens kan vara att beslut fattas grundade på felaktiga grunder och ytterst att den registrerade får felaktigt beslut, eventuellt med rättsverkningar. Utbildning är avgörande för att reducera risken för bias till en acceptabel nivå. En möjlighet kan också vara att i styrdokument fastställa ett förbud mot att använda AI vid vissa beslut. Dessa riskreducerande åtgärder innebär, om de införs, att den planerade behandlingen följer principen om korrekthet.

Sammantaget kan kommunen påvisa hur det är möjligt att de registrerades personuppgifter behandlas på ett rättvist, skäligt och proportionerligt sätt i enlighet med vad de registrerade har anledning att förvänta sig. Situationerna där AI-assistenten tillåts användas har i samtliga fall en stark koppling till respektive förvaltnings eller bolags uppdrag. Behandlingen är därför rimlig i förhållande till ändamålet.

4.1.3 Öppenhet

Principen om öppenhet innebär en skyldighet att säkerställa att personuppgiftsbehandlingen är begriplig och transparent för den registrerade, vilket manifesteras genom informationsskyldigheten. Det skall vara klart och tydligt för den registrerade hur personuppgifter som rör denne behandlas eller kommer att behandlas (skäl 39).

[6] bilaga 3 - riskanalys.xlsx

Varbergs kommun har rutiner på plats för hur de registrerade skall informeras och som gäller även för AI-plattformen. Rätten till information av de personuppgiftsbehandlingar som uppstår vid användandet av Intrics AI-plattform och som är gemensamma för samtliga personuppgiftsansvariga skall delges genom lättillgänglig information på kommunens hemsida. Varje personuppgiftsansvarig, det vill säga varje nämnd och styrelse har ett eget ansvar att informera de registrerade om bland annat vilka personuppgifter som behandlas och vilka kategorier av mottagare som får tillgång till deras personuppgifter.

Eftersom kommunens personuppgiftsansvariga har vitt skilda verksamheter behöver de var för sig kartlägga hur de avser att använda AI-plattformen. Om det avviker från den gemensamma informationen skall det framgå av informationen på förvaltningens hemsida. Detta förfarande möjliggör för de registrerade att vända sig till respektive nämnd eller bolag för att få ytterligare information om så önskas. Det finns således goda möjligheter för de registrerade att informera sig om hur deras personuppgifter behandlas. Därför är behandlingen transparent gentemot de registrerade.

4.1.4 Ändamålsbegränsning (artikel 5.1. b)

Personuppgifter får enbart behandlas om de samlats in för särskilda, uttryckligt angivna och berättigade ändamål (artikel 5.1b). De specifika ändamål som personuppgifterna behandlas för bör vara tydliga, legitima och bör ha bestämts före behandlingen påbörjas (skäl 39).

Ändamålsbegränsningen har ombesörjts genom en processkartläggning, varvid ett begränsat antal specifika ändamål identifierades och dokumenterades (sid. 12). Vid processkartläggningen bröts processen ned till en nivå som förklarar hur informationen flödar mellan kommunen och leverantören. Detta för att säkerställa att de angivna ändamålen är specifika, det vill säga att ändamålen är preciserade så långt som det är möjligt.

Processerna som identifierades bedöms i olika utsträckning kunna förekomma i samtliga förvaltningar och bolag. Behandlingens ändamål är begränsad till processkartläggningen. Och det är troligt att de personuppgiftsansvariga i stort delar samma ändamål. De personuppgiftsansvariga som avser att använda AI-plattformen behöver dokumentera behandling och ändamål i sina behandlingsregister, samt vid behov göra anpassningar innan behandlingen påbörjas.

Slutsatsen är att ändamålsbegränsningen är säkerställd genom processkartläggningen och de förhandsvillkor som föreskriver dokumentation per personuppgiftsansvarig i avsnitt 8.

4.1.5 Uppgiftsminimering (artikel 5.1 c)

Personuppgifter skall vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (artikel 5.1 c). Principen är ett uttryck för proportionalitetstanken inom dataskyddsrätten, vilket innebär att de uppgifter som behandlas skall vara begränsade till att inte omfatta mer än vad som behövs för att uppnå syftet med behandlingen.

I den planerade behandlingen är uppgiftsminimeringen en av de mer utmanande principerna att efterleva, eftersom AI-plattformen tekniskt sett möjliggör för användaren att tillföra en obegränsad mängd material i en prompt eller kunskapssamling.

Den faktiska uppgiftsminimeringen sker i två led. Dels på systemnivå genom de begränsningar Intric på uppdrag av kommunen tillämpar avseende lagring, gallring och säkerhetsklassning, dels på användarnivå genom kommunens utbildningsprogram som ingår i AI-policyn.

Leverantörens behörighetshantering säkerställer vilka uppgifter som specifika användare i produktionsmiljön får tillgång till. Som utgångspunkt tillämpas begränsad produktionstillgång, där endast en (1) person har full åtkomst till produktionsmiljön.

Åtkomsten till plattformen är rollbaserad, vilket innebär att kommunen har full kontroll över dataflödet. En person i Varbergs kommun tilldelas ansvar för dataflödet och skall på uppdrag av kommunen, tillsammans med leverantören, begränsa åtkomsten till exempelvis olika AI-modeller. Åtkomstminimeringen bidrar dels till att eliminera personuppgiftsbehandlingar som är problematiska ur ett dataskyddsperspektiv, dels möjliggöra för förvaltningar och verksamheter att avstå från att tillåta exempelvis tillgång till vissa ”spaces” och minska risken för mänskliga misstag.

En förutsättning för medarbetare att få tillgång till AI-plattformen är att de har genomgått en utbildning och bedömts ha tillräckliga dataskyddskunskaper för att med hög tillförlitlighet kunna tillämpa uppgiftsminimering.

Endast de personuppgifter som är relevanta får behandlas. När uppgifterna inte längre är relevanta skall de raderas av användaren utan onödigt dröjsmål.

Radering kommer även att ske automatiskt i enlighet med de tidsfrister som kommunen beslutar. Genom att tillämpa automatisk gallring elimineras risken för att uppgifter samlas in och lagras med argumentet att de eventuellt kan komma till nytta i framtiden.

AI-assistenten samlar endast in de personuppgifter som är absolut nödvändiga för att tillhandahålla tjänsten. Användarna kommer att utbildas dels om de

inbyggda riskerna med AI-användande såsom bias, dels gällande den kontext och omfattning i vilken personuppgifter får användas.

AI-assistenten tillämpar aktiv lagringsminimering vilket bidrar till att säkerställa att personuppgifterna inte är överflödiga eller sparas längre än nödvändigt. Detta är en inbyggd del i systemdesignen.

Kommunen har genom styrdokument implementerat organisatoriska skyddsåtgärder som syftar till att personuppgifter ska behandlas med de registrerades rättigheter i åtanke, och ej i större omfattning än vad som är nödvändigt.

Slutsatsen är att de tekniska och organisatoriska åtgärderna sammantaget bedöms säkerställa principen.

4.1.6 Riktighet (artikel 5.1 d)

GDPR artikel 5.1 d stipulerar att personuppgifter skall vara riktiga och om nödvändigt uppdaterade. Det innebär att personuppgifter som inte stämmer skall utan dröjsmål rättas eller raderas.

AI-plattformen är avsedd att fungera som ett stöd för medarbetare i fullföljandet av olika arbetsuppgifter som överensstämmer med de ändamål som har angivits. Den utdata som AI-plattformen genererar granskas därför omedelbart av användaren i samband med att arbetsuppgiften utförs. Felaktigheter i utdata avvisas omedelbart varvid nya utdata genereras. Processen upprepas tills utdata är korrekt. Om önskat resultat inte kan uppnås förkastas utdata i sin helhet och arbetsuppgiften utförs manuellt. Slutsatsen är att riktigheten både kontrolleras korrigeras omedelbart.

AI-plattformen är inte avsedd att användas som lagringsyta, vilket innebär att korrigering av riktigheten utöver vad som beskrivs ovan inte är relevant. Den beskrivna feedbackloopen mellan användare och AI-plattform bedöms vara en adekvat och proportionerlig åtgärd för säkerställande av personuppgifternas riktighet i förhållande till behandlingens ändamål.

4.1.7 Lagringsminimering (artikel 5.1 e)

Enligt GDPR artikel 5.1 e får personuppgifter inte behandlas i en form som möjliggör identifiering av den registrerade under längre tid än vad som är nödvändigt för personuppgiftsbehandlingens ändamål. Lagringstiden måste därmed motiveras utifrån syftet med behandlingen och säkras genom rutiner för gallring. Artikeln ger uttryck för principen om lagringsminimering.

Lagringsminimeringen kommer att säkerställas genom att användarna utbildas i vikten av att inte spara uppgifterna längre än vad som är nödvändigt för att uppfylla det ändamål för vilket personuppgifterna samlades in. Användarna

kommer att få tekniskt stöd genom att uppgifterna raderas automatiskt. Den automatiska raderingen sker enligt tidsfrister som är fastställda i respektive personuppgiftsansvariges dokumenthanteringsplan. Implementeringen av tidsfristerna i enlighet med dokumenthanteringsplan utförs av AI-plattformens utsedda AI-administratör i samverkan med respektive verksamhet.

Den automatiska raderingen är också en vital säkerhetsåtgärd i händelse av att en användare uppsåtligen eller av misstag inte respekterar de instruktioner som skall säkerställa lagringsminimering.

Slutsatsen är att tekniska och organisatoriska åtgärder sammantaget skapar förutsättningar för att principen om lagringsminimering efterlevs utifrån de modeller och användarfall som är aktuella för den planerade behandlingen.

4.1.8 Integritet och konfidentialitet (artikel 5.1 f)

Artikel 5.1 f fastslår att personuppgifter skall behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna. Kraven omfattar skydd som innebär att endast behöriga har tillgång till personuppgifterna, att de är korrekta och skyddas mot avsiktlig eller oavsiktlig ändring eller förstörelse.

Artikel 32 p. 1 operationaliserar principen genom att specificera vad som ryms i begreppet lämplig säkerhet. Personuppgiftsansvarige och personuppgiftsbiträdet skall vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämpligt i förhållande till risken. Exempel på åtgärder kan vara pseudonymisering, kryptering, förmåga att säkerställa konfidentialitet, integritet och tillgänglighet, incidenthantering och systematiskt informationssäkerhetsarbete.

Intric AB har redogjort för de som säkerhetsåtgärder som vidtagits på organisatorisk nivå såväl som för säkerheten i AI-plattformen. Nedan, en sammanfattning över de viktigaste åtgärderna.

Organisatoriska säkerhetsåtgärder

Intric AB, är certifierad enligt ISO 27001:2022, vilket indikerar att Intric som organisation har implementerat ett ledningssystem för informationssäkerhet. Certifieringen innebär att Intric kan påvisa att informationssäkerhetsarbetet följer vedertagen praxis och att informationssäkerheten följs upp genom extern revision. En granskning av ledningssystemets SOA ger vid handen att det har en hög implementeringsgrad gällande de obligatoriska säkerhetsåtgärderna i ISO 27001:2022, Annex A. Enligt protokollet har samtliga åtgärder som är relevanta för Intrics verksamhet har implementerats. Detta inkluderar:

- styrdokument
- utpekade roller och ansvar

- utbildning
- kontroll av regelefterlevnad
- dokumentation
- process för avvikelsehantering
- avtalsuppföljning
- leverantörskontroller
- riskhantering
- incidenthantering
- intern revision
- extern revision
- ständiga förbättringar
- kontinuitetsarbete inklusive övning
- regler och rutiner för behörighetshantering

Tillsammans utgör de organisatoriska åtgärderna kärnan i systematiskt informationssäkerhetsarbete. Slutsatsen är att Intric kan påvisa att de har vidtagit lämpliga organisatoriska skyddsåtgärder i förhållande till de risker som organisationen hanterar.

Tekniska säkerhetsåtgärder AI-plattformen

Åtkomstkontroll och Behörighetshantering

- rollbaserad åtkomst (RBAC)
- Single Sign-On (SSO)
- Multifaktorautentisering (MFA)

Kommunen har möjlighet att definiera detaljerade användarroller och begränsa åtkomst till funktioner, dokument och AI-modeller. Inloggning och åtkomst motsvarar den teknik som används inom kommunen och kan integreras fullt ut med kommunens behörighetshantering.

Dataminimering

- val av AI-modell
- dataminimering

Kommunen väljer mellan globala, europeiska, svenska eller lokala språkmodeller baserat på säkerhetskrav. Kommunen konfigurerar vilken data som ska bearbetas och kan begränsa omfattningen. Därtill har AI-plattformen en ”Redaction-funktion”, som kan användas för att aktivt dataminimera personuppgifter i den information som till exempel förekommer i olika spaces.

Kryptering

- end-to-end kryptering
- krypterad lagring
- säkra API-anrop

För kommunen innebär krypteringsfunktionerna att data krypteras både i *transit* och i *rest*. All dokumentation och konversationshistorik lagras krypterat. All kommunikation mellan system sker via krypterade kanaler (TLS 1.2+).

Loggning och Spårbarhet

- export av loggar
- dataåtkomstlogg
- användaransvar

Genomförandet av loggning och spårbarhet sker i enlighet med vägledningar i etablerade standarder. Möjlighet att finns exportera loggar för integration med kommunens SIEM-system. Det inkluderar fullständig loggning av vem som har tillgång till vilken information. Insyn gällande vilken användare som ansvarar över både verktyg/assistent och uppladdad information finns tillgänglig.

Datahantering, radering & backup

- dataägande
- selektiv radering
- massradering
- exportfunktion
- automatisk radering
- automatiska backuper
- återställningsfunktion
- backup

Dataägandet innebär konkret att kommunen behåller full äganderätt till all data i systemet. AI-plattformen har inbyggd funktionalitet att radera all data vid avslut av tjänsten. Kommunen kan exportera all data i strukturerade format. AI-plattformen har konfigurerbara retentionsregler för automatisk radering efter viss tid. Backup genomförs med daglig frekvens av kommunens data. Kommunen kan återställa raderad data inom definierad period.

Nätverkssäkerhet

- sessionstimeout
- lösenordpolicy

Ovanstående säkerhetsåtgärder avseende nätverkssäkerhet bidrar till att stärka dataskyddet genom att övervaka inloggning och inaktivitetstid för automatisk utloggning. Lösenordspolicyn konfigureras i enligt med kommunens krav.

De tekniska och organisatoriska säkerhetsåtgärder som Intric redogör för indikerar att lämpliga säkerhetsåtgärder har implementerats i en omfattning som generellt kan anses motsvara en väl avvägd och lämplig säkerhetsnivå. Den specifika risken utifrån kommunens förutsättningar utgår från den riskanalys som genomförts som en del av denna DPIA.[7] Riskanalysen diskuteras mer ingående i avsnitt 5 nedan. I detta sammanhang är riskanalysen relevant ur ett riskhanteringsperspektiv. Det vill säga, om säkerhetsåtgärderna är tillräckliga för att hantera de risker som föreligger. Riskanalysen identifierar ett antal risker som hanteras i analysen. Riskhanteringen bygger till stor del på de administrativa riskreducerande åtgärderna som kommunen vidtar. Följaktligen är det nödvändigt att åtgärderna implementeras av kommunen för att den önskade effekten skall uppnås.

Slutsatsen är att Intrics säkerhetsåtgärder säkerställer en lämplig säkerhetsnivå enligt vad som avses i artikel 32. Dock inte ensamma, utan givet att kommunen implementerar de riskreducerande åtgärder som redovisas i riskanalysen. Sammantaget kan kommunens och Intrics säkerhetsåtgärder anses säkerställa lämplig skyddsnivå.

4.1.9 Behandling av särskilda kategorier av personuppgifter (artikel 9)

Artikel 9.1 innebär att förbud mot att behandla särskilda kategorier av personuppgifter. Kategorierna får endast behandlas i begränsade undantagsfall, i kombination med nationell rätt och lämpliga skyddsåtgärder.

Den planerade behandlingen omfattar särskilda kategorier av personuppgifter enligt artikel 9.1, närmare bestämt uppgifter som avslöjar etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, uppgifter om hälsa, samt uppgifter om sexualliv eller sexuell läggning. Huvudregeln är, som nämnt ovan, att behandling av sådana uppgifter är förbjuden om inte något av de undantag som redogörs i artikel 9.2 är tillämpligt.

Förbudet mot behandling av särskilda kategorier av personuppgifter motiveras av att sådana uppgifter typiskt sett är särskilt skyddsvärda för den enskildes integritet. Av detta följer att den som vill behandla dessa uppgifter måste kunna åberopa ett av undantagen i artikel 9.2. Det är inte tillräckligt att det finns en rättslig grund för behandlingen enligt artikel 6. Med andra ord, behandlingen kräver både rättslig grund enligt artikel 6 och undantag som uttryckts i artikel 9.2.

[7] bilaga 3 - riskanalys.xlsx

Relevanta undantag som kan åberopas för kommunal verksamhet

Av de tio undantagen i artikel 9.2 bedöms fyra kunna vara relevanta för en kommunal verksamhet:

- artikel 9.2 b, arbetsrätt och social trygghet
- artikel 9.2 g, väsentligt allmänt intresse
- artikel 9.2 h, hälso- och sjukvård samt social omsorg
- artikel 9.2 j, arkivändamål av allmänt intresse.

Dessa undantag förutsätter att behandlingen är förankrad i unionsrätt eller nationell rätt. Den svenska kompletterande regleringen finns i 3 kap. dataskyddslagen (2018:218), mer specifikt i 3 kap. §§ 2, 3, 5 och 6 (arbetsrätt, väsentligt allmänt intresse, hälso- och sjukvård samt social omsorg, arkivändamål).

Relevanta är även de sektorsspecifika registerförfattningar som operationaliserar undantagen för respektive verksamhetsområde. Dessa är patientdatalagen (2008:355) för hälso- och sjukvård, lagen(2001:454) om behandling av personuppgifter inom socialtjänsten (SoLPUL) jämte förordningen (2001:637) om behandling av personuppgifter inom socialtjänsten (SoLPUF) för socialtjänsten, samt arkivlagen(1990:782) för arkivverksamhet.

Vid behandling inom förskola, grundskola eller annan skolverksamhet, tillämpas skollagen (2010:800) särskilt 26 a kap. samt förordning (2018:1366) om sökbegränsningar i skolan. Vid behandling inom skolhälsovården gäller även patientdatalagen.

Nödvändighetskravet

Samtliga undantag som åberopas förutsätter att behandlingen är nödvändig för det aktuella ändamålet. Av rättspraxis följer att nödvändighetskravet är strikt: behandlingen skall vara den minst integritetskränkande tillgängliga åtgärden för att uppnå ändamålet.[8] För kommunens del gällande AI-plattformen innebär det att behandling av känsliga personuppgifter får ske där andra metoder inte är tillräckliga.

Tillämpning i denna DPIA

Eftersom scopet på denna DPIA är kommunens samtliga nämnder och bolag, kan den inte fastställa ett specifikt undantag i artikel 9.2 som täcker all behandling. Detta på grund av att kommunens verksamheter har olika underliggande

[8] EU-domstolens dom av den 1 augusti 2022, *OT mot Vyriausioji tarnybinės etikos komisija,* C-184/20, EU:C:2022:601

rättsliga grunder. Därav följer att valet av undantag måste göras per användningsfall.

Med anledning av detta åligger det respektive personuppgiftsansvarig nämnd eller bolag att före påbörjandet av en behandling av känsliga personuppgifter dokumentera följande i sitt behandlingsregister:

1. det specifika ändamålet för behandlingen
2. den rättsliga grunden enligt artikel 6
3. vid behandling inom hälso- och sjukvård eller socialtjänst, hänvisning till tillämpliga registerförfattningar
4. en bedömning av nödvändighet i det enskilda användningsfallet

Denna dokumentation utgör en av förutsättningarna för att plattformen får aktiveras för respektive personuppgiftsansvarig och regleras som förhandsvillkor i avsnitt 8.

4.2 De registrerades rättigheter

Klart och tydlig information (artikel 12-14)

Den personuppgiftsansvarige är skyldig att vidta lämpliga åtgärder för att informera den registrerade om behandlingen. Informationen skall vara koncis, klar, begriplig och lättillgänglig med ett klart och tydligt språk (artikel 12). Informationen skall omfatta uppgifter om vilka personuppgifter som samlas in från den registrerade (artikel 13). Samt vilka personuppgifter som samlats in från någon annan än den registrerade (artikel 14).

Personuppgifterna som samlas in för att behandlas i AI-plattformen består av information som användaren antingen skriver eller promptar i AI-plattformen. Alternativt laddar användaren upp material som innehåller personuppgifter. Förutom de personuppgifter som användaren aktivt lämnar till AI-plattformen, behandlas användarens inloggningsuppgifter. Dessa härrör från kommunens AD-inloggning. De registrerade vilkas personuppgifter samlas in och behandlas i AI-plattformen kommer att informeras via kommunens hemsida. Användarna av AI-plattformen informeras om behandlingen via kommunens intranät samt i samband med den obligatoriska utbildning användarna genomgår före användande av AI-plattformen.

Tillgång (artikel 15)

Den registrerade har enligt artikel 15 rätt att få en bekräftelse huruvida personuppgifter som rör denne behandlas. Huvudregeln är att den registrerade, om personuppgifter behandlas, har rätt till att få tillgång till personuppgifterna (artikel 15.1).

Rätten till tillgång är inte en absolut rättighet. I Sverige regleras undantag i Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning

(dataskyddslagen). I 5 kap. 2 § 1 st. dataskyddslagen finns ett undantag som innebär att artikel 15 i dataskyddsförordningen inte gäller personuppgifter i löpande text som inte fått sin slutliga utformning när begäran gjordes eller som utgör minnesanteckning eller liknande. Enligt 2 § 2 st. gäller dock inte undantaget om personuppgifterna:

1. har lämnats ut till tredje part
2. behandlas enbart för arkivändamål av allmänt intresse eller statistiska ändamål, eller
3. har behandlats under längre tid än ett år i löpande text som inte har fått sin slutliga utformning.

AI-plattformen är utformad som ett verktyg specifikt för att bearbeta och förädla material i olika sammanhang. Slutprodukten är i samtliga fall ett utkast. Utkastet granskas och färdigställs av användaren. Man skulle kunna argumentera för att undantaget i 5 kap. 2 § 1 st. tillämpligt. Argumenten bygger på att användaren raderar underlagen från AI-plattformen när utkastet är klart eller har utlämnats, samt att arbetet inte pågår längre än ett år och att kvarhållningsprinciperna i AI-plattformen forcerar en gallring inom ett år från arbetet påbörjande, är undantaget tillämpligt. Följaktligen skulle inte den tilltänkta behandlingen omfattas av rätten till tillgång enligt artikel 15.

Detta är dock ett resonemang som bygger på ett stort tolkningsutrymme. Argument som talar emot tolkningen är att undantaget historiskt har avsett anteckningar i löpande arbete. Huruvida AI-genererad text faller in under begreppet ”minnesanteckning eller liknande” är inte rättsligt prövat.

Slutsatsen är att rättsläget i den tilltänkta behandlingen är oklart. Personuppgiftsansvarige bör därför vara beredd att hantera en specifik begäran om tillgång enligt artikel 15, även om man väljer att generellt åberopa undantaget. Därav av följer att verksamheterna behöver ta höjd för att hantera rätten till tillgång i den behandling som sker i AI-plattformen.

Rättelse (artikel 16)

Den registrerade har rätt att få felaktiga uppgifter rättade, dock med beaktande av ändamålet med behandlingen (artikel 16). Eftersom ändamålet med behandlingen är begränsat till att på olika sätt assistera användaren med att färdigställa material utan att lagra den färdiga produkten, är det inte aktuellt att rätta eventuellt felaktiga personuppgifter.

Radering (artikel 17)

Grundregeln i artikel 17 är att den registrerade har rätt att vid begäran få sina personuppgifter raderade. Den rättsliga grunden för behandlingen är allmänt intresse. Behandlingar som sker för att utföra en uppgift av allmänt intresse är undantagna regeln vilket således innebär att den personuppgiftsansvarige kan neka en begäran om radering i de fall behandlingen är nödvändig för att utföra uppgiften av allmänt intresse (artikel 17.3 b). Avslag förutsätter att nödvändighetsrekvisitet bedöms i det enskilda fallet eftersom inte allt nyttjande av AI-plattformen når den tröskeln

Begränsning av behandling (artikel 18)

Den registrerade har enligt artikel 18 GDPR rätt att under vissa omständigheter begära att behandlingen av dennes personuppgifter begränsas. Rätten gäller i de fall som anges i artikel 18.1 a-d, exempelvis om den registrerade bestrider personuppgifternas korrekthet eller om behandlingen är olaglig men den registrerade motsätter sig radering och i stället begär begränsning. I den planerade behandlingen finns ingen generell grund för att utesluta tillämpningen av artikel 18. Rätten gäller formellt. I praktiken blir den dock sällan aktuell eftersom personuppgifterna gallras snabbt och behandlingen är temporär. Det vill säga utdata granskas av användaren vartefter underlaget raderas. Vid en konkret begäran om begränsning ska personuppgiftsansvarig nämnd eller bolag göra en bedömning utifrån omständigheterna i det enskilda fallet.

Den registrerades rimliga förväntningar ska bedömas med hänsyn till relationen mellan denne och den personuppgiftsansvarige, samt den kontext i vilken personuppgifterna behandlas.

Dataportabilitet (artikel 20)

Personuppgifterna raderas snarast möjligt efter att användaren granskat det material som AI-plattformen genererat. Personuppgifterna förekommer dessutom i löpande text och ostrukturerat på ett sätt som utesluter dataportabilitet. Dataportabilitet är inte möjligt i den aktuella behandlingen.

Rätt att invända (artikel 21)

När den rättsliga grunden för behandlingen är uppgift av allmänt intresse enligt artikel 6.1.e GDPR har den registrerade enligt artikel 21.1 rätt att av skäl som hänför sig till dennes specifika situation invända mot behandlingen. Den personuppgiftsansvarige får i en sådan situation inte längre behandla personuppgifterna såvida den personuppgiftsansvarige inte påvisar tvingande berättigade skäl för behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter. Vid en eventuell invändning ska respektive personuppgiftsansvarig nämnd eller bolag göra en avvägning i det enskilda fallet

Att inte bli föremål för automatiserat beslutsfattande (artikel 22)

De registrerades personuppgifter kommer inte att bli föremål för automatiserat beslutsfattande. Allt material, inklusive eventuella beslutsförslag granskas manuellt.

4.3 Skyddsåtgärder för internationella överföringar

Den planerade behandlingen omfattar inga överföringar av personuppgifter till tredje land. Samtliga aktiverade underbiträden för känsliga personuppgifter har lokalisering i Sverige (GleSys AB, AI Iron AB, Berget AI AB).

Underbiträden inom EU/EES vars behandling inte aktiveras för känsliga personuppgifter (Verda Oy i Finland, LinkUp och Scaleway i Frankrike) säkerställs vara deaktiverade genom säkerhetsklassningsfunktionen i AI-plattformen. Kapitel V GDPR aktualiseras därmed inte.

För en utförligare redogörelse, se avsnitt 3.2 tabell 2 samt avsnitt 8 förhandsvillkor.

4.4 Behandling utförd av personuppgiftsbiträde.

När behandlingen av personuppgifter utförs av någon annan än den personuppgiftsansvarige själv inträder bestämmelserna i artikel 28 GDPR. Bestämmelsen kräver att den personuppgiftsansvarige endast anlitar personuppgiftsbiträden som ger tillräckliga garantier om att lämpliga tekniska och organisatoriska åtgärder genomförs på ett sådant sätt att behandlingen uppfyller dataskyddsförordningens krav och säkerställer skyddet för de registrerades rättigheter. Behandlingen skall regleras genom ett skriftligt personuppgiftsbiträdesavtal som omfattar de villkor som räknas upp i artikel 28.3.

I den planerade behandlingen är Intric AB personuppgiftsbiträde till de personuppgiftsansvariga nämnder och bolag i Varbergs kommun som behandlar känsliga personuppgifter i AI-plattformen.

Atea Sverige AB är leverantör enligt det leveransavtal, (Egen upphandling KS 23/15), som är tillämpligt för leveransen, men är inte personuppgiftsbiträde.[9]

Personuppgiftsbiträdesavtalet är direkt mellan kommunen och Intric AB.

[9] Avtal AI-plattform Intric (KS 2024/0609-11)

Gällande avtal och avtalets räckvidd

Det gällande personuppgiftsbiträdesavtalet med Intric AB baseras på SKR:s avtalsmall version 2.1 (2023-04-06) och uppfyller formellt kraven i artikel 28 för icke-känsliga personuppgifter.[10] Avtalet inkluderar bilaga 1 med instruktion för behandlingen samt bilaga 2 med förteckning över godkända underbiträden. Genomgång av avtalet visar att samtliga obligatoriska delmoment enligt artikel 28.3 omfattas:

instruktioner från personuppgiftsansvarig, tystnadsplikt, säkerhetsåtgärder, anlitande av underbiträden, bistånd vid uppfyllande av personuppgiftsansvariges skyldigheter, radering eller återlämnande vid avtalets upphörande, samt rätt till granskning.

Avtalet är dock ingånget med utgångspunkt från att kommunen inte skulle använda AI-plattformen för känsliga personuppgifter. För den planerade behandlingen av känsliga personuppgifter behöver avtalet revideras eller kompletteras. Detta hanteras genom det förhandsvillkor som anges i avsnitt 8.

Underbiträden enligt artikel 28.2 och 28.4

Personuppgiftsbiträdet får anlita underbiträden endast efter förhandsgodkännande från den personuppgiftsansvarige, och underbiträdet är skyldigt att uppfylla samma skyldigheter som personuppgiftsbiträdet.

Enligt bilaga 2 i gällande PUB-avtal är fyra underbiträden godkända:

GleSys AB, Airon (varumärke), DataCrunch Oy och Berget AI AB. Genom korrespondens med Intric AB (2026-05-07) har det bekräftats att AI Iron AB (organisationsnummer 559490-8054) är den juridiska enhet som tillhandahåller GPU-kapacitet för språkmodeller; varumärket Airon härrör från en tidigare leverantörskonstellation där Ember AB var avtalspart, vilket inte längre är aktuellt. DataCrunch Oy har bytt firmanamn till Verda Oy med bibehållet organisationsnummer.

För behandling av känsliga personuppgifter är de aktiverade underbiträdena GleSys AB (infrastruktur, Sverige), AI Iron AB (språkmodeller, Sverige) och Berget AI AB (transkribering och embedding, Sverige). Övriga underbiträden — Verda Oy i Finland, LinkUp i Frankrike och Scaleway i Frankrike — är deaktiverade för behandling av känsliga personuppgifter genom säkerhetsklassningen i AI- plattformen.

Tystnadspliktsskyddet hos personuppgiftsbiträdet

Artikel 28.3 b kräver att personuppgiftsbiträdet säkerställer att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt. För Intric AB:s personal aktualiseras i den planerade behandlingen lag (2020:914) om

[10] PUB-avtal Intric (KS 2024/0609-15)

tystnadsplikt vid utkontraktering. Lagen innebär att den som på grund av anställning eller uppdrag hos personuppgiftsbiträdet deltar i behandlingen av sekretessbelagda uppgifter omfattas av samma tystnadsplikt som om uppgiften hade behandlats inom myndigheten. Brott mot tystnadsplikten är straffsanktionerat enligt 20 kap. 3 § brottsbalken.

Sedan 1 juli 2023 är meddelarfriheten inskränkt för personal hos personuppgiftsbiträden som behandlar uppgifter på uppdrag av myndighet (prop. 2022/23:97). Tillsammans utgör dessa bestämmelser ett rättsligt skydd som i materiellt hänseende motsvarar det som gäller för kommunens egen personal.

Vidare innebär gällande PUB-avtals avsnitt 8 att samtliga personer som arbetar under Intrics ledning är bundna av sekretessförbindelse avseende behandlingen om de inte redan omfattas av straffsanktionerad lagstadgad tystnadsplikt. Avtalets bilaga 1 punkt 9 namnger Jonatan Cerwall (CTO) som den enda person hos Intric med tillgång till produktionsdatabasen, och byte av sådan person kräver kommunens skriftliga medgivande. Detta är en skarp organisatorisk åtgärd som tydligt begränsar kretsen av personer med faktisk åtkomst.

Säkerhetsåtgärder och granskning

De säkerhetsåtgärder som Intric vidtagit har redogjorts för i avsnitt 4.1.8. Intric är certifierat enligt ISO/IEC 27001:2022 och granskningen av Statement of Applicability visar hög implementeringsgrad av relevanta säkerhetsåtgärder enligt Annex A. Personuppgiftsansvarig har enligt avsnitt 9 i PUB-avtalet rätt att själv eller genom utsedd tredje part följa upp att personuppgiftsbiträdet uppfyller avtalets, instruktionens och dataskyddslagstiftningens krav.

Sammantagen bedömning av personuppgiftsbiträdes behandling

Personuppgiftsbiträdesförhållandet uppfyller kraven i artikel 28 GDPR under förutsättning att gällande avtal revideras eller kompletteras med utgångspunkt från behandling av känsliga personuppgifter, och att bilaga 2 över godkända underbiträden uppdateras så att samtliga aktiva underbiträden upptas. Tystnadspliktsskyddet hos personuppgiftsbiträdet bedöms tillräckligt genom lag (2020:914), avtalets sekretessbestämmelser och den begränsade kretsen av personer med produktionsåtkomst. Avtalsuppföljning sker inom ramen för kommunens ordinarie leverantörsuppföljning enligt avsnitt 10.

4.5 Sammantagen rättslig bedömning

Den rättsliga analysen visar att det finns en rättslig grund för behandlingen enligt artikel 6.1 e GDPR och att de undantag som kan åberopas för känsliga personuppgifter enligt artikel 9.2 GDPR är förankrade i nationell rätt.

Dataskyddsprinciperna kan följas, behandlingen bedöms nödvändig och proportionerlig, och de registrerades rättigheter kan tillgodoses.

Den rättsliga bedömningen förutsätter att de förhandsvillkor som anges i avsnitt 8 är uppfyllda. Detta gäller särskilt revidering av huvudavtal och PUB-avtal med utgångspunkt från behandling av känsliga personuppgifter, bekräftelse från respektive personuppgiftsansvarig om avgränsning mot sekretess, teknisk konfiguration av säkerhetsklassningen, fullföljd användarutbildning samt dokumenterat ställningstagande till artikel 9.2-undantag per användningsfall.

Sammantaget bedöms den planerade behandlingen uppfylla de rättsliga kraven under förutsättning att förhandsvillkoren genomförs. Avvikelse från förhandsvillkoren förändrar bedömningen och kan föranleda kompletterande DPIA enligt avsnitt 3.1

Som framgår av riskanalysen och den strukturella observationen i avsnitt 5.2 är AI-administratörens funktion och säkerhetsklassningen centrala för att förhandsvillkoren ska få praktisk verkan. Detta innebär att den rättsliga bedömningen är beroende inte enbart av att förhandsvillkoren formellt uppfylls vid driftsättning, utan också av att de upprätthålls över tid genom kontinuerlig uppföljning enligt avsnitt 10.

5. Riskhantering

5.1 Identifiering av riskerna

Riskanalys har genomförts i vilken 50 risker har identifierats och analyserats.[11] Matrisen nedan i Figur 4, illustrerar riskerna före respektive efter riskreducerande åtgärder genomförts. Före implementering av riskreducerande åtgärder bedöms 11 av de identifierade riskerna kunna ge allvarliga konsekvenser för de registrerades rättigheter. Efter riskreducerande åtgärder bedöms två av de kvarstående riskerna, Riskid #21 och #23, ha så pass högt riskvärde att de kan medföra allvarliga konsekvenser för de registrerade.

Riskid #21 utgörs av ett antagonistiskt angrepp mot AI-plattformen, där personuppgifter exfiltreras från AI-plattformen, vilket medför att obehöriga får åtkomst till känsliga personuppgifter. Riskid #23 består av att obehörig får åtkomst till personuppgifterna i utskriven form genom fysisk åtkomst. Sårbarheten består av felaktig förvaring. Sannolikheten för att Riskid #21 och #23 skall realiseras efter att riskreducerande åtgärder vidtagits bedöms som låg, mer sällan än en gång per 10 år.

Samtliga återstående risker som har värderats har en risknivå efter riskreducerande åtgärder som generellt bedöms vara acceptabla enligt den valda riskvärderingsmodellen. Riskerna med Riskid #2, #12, och #20 har högst risk,

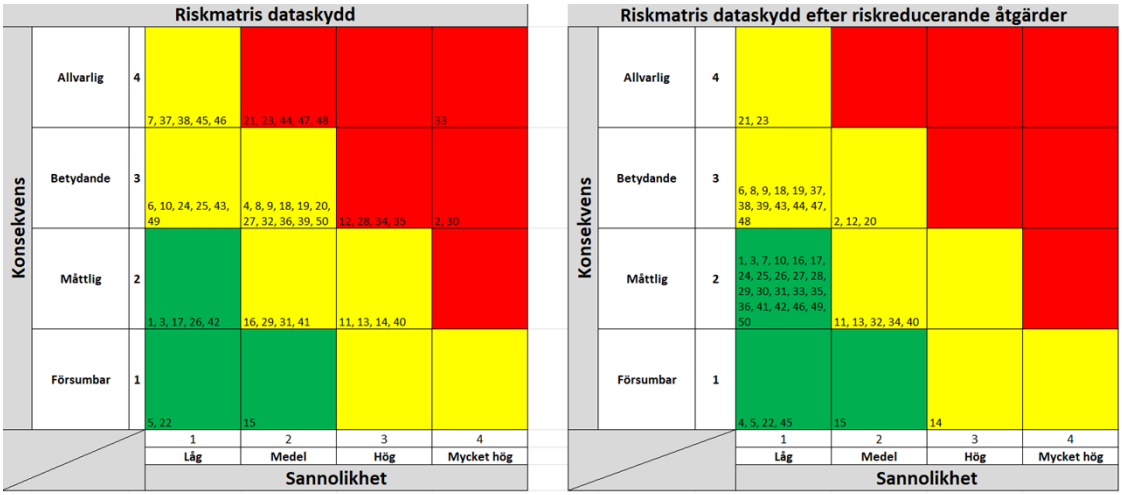
[11] bilaga 3 - riskanalys.xlsx

riskvärde 6. Sannolikheten för att dessa risker skall realiseras bedöms som medelhög. Den förväntade frekvensen är mellan en gång per år till en gång per tio år.

Riskid #2 har sitt ursprung i felaktigt användande av USB-minne, där känsliga personuppgifter sparas från AI-plattformen till USB-minnet, vilket kan leda till förlust eller obehörig åtkomst av personuppgifter.

Riskid #12 är en oönskad händelse där information ändras på grund av mänskligt fel eller misstag. En konsekvens kan vara att information som innehåller personuppgifter förlorar sin riktighet.

Riskid #20 är kopplat till antagonistiskt angrepp där sårbarheter hos användarna på olika sätt exploateras. Medarbetare utsätts för social engineering-attack, phishing-attack, utpressning eller motsvarande, som leder till att hotaktören får tillträde till AI-plattformen. Konsekvensen om risken realiseras är att information manipuleras. Vilket resulterar i att information som innehåller personuppgifter förlorar sin riktighet.



Figur 4: Riskmatris före- respektive efter riskreducerande åtgärder genomförts.

5.2 Strukturell observation från riskanalysen

Riskanalysen redovisar identifierade risker enskilt med tillhörande åtgärder. När åtgärderna däremot betraktas samlat, på det sätt som det gör vid analystillfället, framträder ett mönster som inte är synligt på enskild risknivå, men som är centralt för bedömningen av behandlingens tillåtlighet.

Av de identifierade riskerna är AI-administratören riskbärande åtgärd i 18 av 50 risker, varav i sex av de sju risker som har högst riskvärde före åtgärd. Säkerhetsklassningsfunktionen i AI-plattformen, det vill säga den tekniska spärr som AI-administratören ansvarar för, återkommer som riskreducerande åtgärd i ett ännu större antal risker, både för risker direkt kopplade till avgränsningen

mot sekretess och för risker rörande felaktig användning, gallring, åtkomststyrning och hantering av underbiträden.

Innebörden är att AI-administratörens funktion tillsammans med säkerhetsklassningen utgör den strukturella grund som gör behandlingen praktiskt möjlig. Om dessa två element fungerar som avsett kan en stor del av riskerna reduceras till en för de registrerade acceptabel nivå.

Även det motsatta gäller. Till exempel om AI-administratören är frånvarande, om rutinerna inte följs eller om säkerhetsklassningen är felkonfigurerad, då försvagas riskreduceringen brett över hela analysen samtidigt.

Det innebär också att riskreduceringen inte främst är beroende av en lång rad oberoende åtgärder, utan av att ett mindre antal centrala funktioner upprätthålls över tid. Detta gör behandlingen möjlig, men det gör den också känslig för bortfall i just dessa funktioner. Denna slutsats påverkar därför utformningen av förhandsvillkoren i avsnitt 8 och uppföljningen i avsnitt 10. Detta gör det väsentligt att AI-administratörens funktion är personoberoende, att rutiner finns för vikariat, delegering. Det är också av stor vikt att GDPR-samordnaren regelbundet följer upp att den funktion som AI-administratören utför för respektive personuppgiftsansvariges räkning, blir verkligen utförd som avsett. Denna fråga hanteras i avsnitt 10.

7. Synpunkter från berörda

7.1 Rekommendationer från dataskyddsombudet

Dataskyddsombudet har inkommit med yttrande 2026-06-09.[12] Yttrandet har granskats och dataskyddsombudets råd har beaktats. Dataskyddsombudet har bekräftat att konsekvensbedömningen följer en ändamålsenlig metod och uppfyller formkraven enligt artikel 35.

Hur respektive råd omhändertas, samt de avvikelser som föreligger jämte motivering för dessa, redovisas i separat bilaga[13]. Bilagan diarieförs tillsammans med konsekvensbedömningen.

7.2 Synpunkter från de registrerade

Samråd har skett internt i central samverkansgrupp (CSG), 2026-04-23.[14] I samband med redovisning av nyligen genomförd pilot gällande Intric AI-

[12] bilaga 6 – samråd dataskyddsombud (KS 2026/0196-7)
[13] bilaga 7 - bemötande av dataskyddsombudets yttrande (2026/0196-8)
[14] Protokoll från central samverkansgrupp (KS 2026/0012-4)

assistent för öppen och harmlös information, uttrycktes att AI har en allt större roll i hur information produceras, distribueras och tolkas. Detta ställer nya krav på kunskap och förståelse hos både individer och organisationer. För att möta dessa utmaningar framfördes bland att kommunen i sitt arbete bör verka för en sammanhållen strategi där medie- och informationskunnighet samt AI-utbildning integreras och förstärker varandra.

7.3 Synpunkter från övriga intressenter

Inga ytterligare samråd har genomförts inom ramen för denna DPIA. Vid framtida väsentliga förändringar i behandlingen som påverkar registrerade kategorier eller behandlingens natur kommer kompletterande samråd att övervägas.

8. Sammantagen bedömning, förhandsvillkor

Den rättsliga analysen i avsnitt 4 och riskhanteringen i avsnitt 5 visar att den planerade behandlingen av känsliga personuppgifter i Intrics AI-plattform kan vara förenlig med dataskyddsförordningens krav. Detta förutsätter dock att ett antal förhandsvillkor är uppfyllda och att dessa upprätthålls över tid.

Intric har påvisat att leverantören arbetar systematiskt med säkerhet, organisatoriskt såväl som tekniskt, och AI-plattformen bedöms tillhandahålla tillräcklig säkerhet i förhållande till de risker som behandlingen medför. Riskanalysen identifierar femtio risker. Förslag på riskreducerande åtgärder finns dokumenterade i bilaga 3.

En central observation i riskanalysen är att en betydande del av de riskreducerande åtgärderna förutsätter att kommunen själv har en fungerande administration av säkerheten i plattformen, i synnerhet rollen som AI-administratör och den tekniska säkerhetsklassningen som funktionen ansvarar för. Om denna administration inte fungerar som avsett återintroduceras ett stort antal risker samtidigt. Detta innebär att riskreduceringen vilar på ett mindre antal centrala funktioner som måste upprätthållas över hela behandlingens livscykel, snarare än på en lång rad av varandra oberoende åtgärder.

Av detta följer att en holistisk hantering krävs där tekniska spärrar, avtalsmässiga förutsättningar och organisatoriska åtgärder samverkar. De förhandsvillkor som anges nedan utgör tillsammans den ram som gör behandlingen möjlig att genomföra på ett sätt som är förenligt med de registrerades rättigheter och friheter. Ansvaret för att förhandsvillkoren uppfylls ligger hos respektive personuppgiftsansvarig nämnd eller bolag, och kontrollen av att de faktiskt är uppfyllda ligger hos AI-administratören inför aktivering av plattformen för den personuppgiftsansvariges räkning.

Förhandsvillkor och tekniska spärrar för driftsättning

DPIA:n är avgränsad till behandling av känsliga personuppgifter som inte omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400). För att avgränsningen skall få avsedd verkan krävs att den tillämpas operativt i samband med driftsättningen.

Spärrarna skall förstås som administrativa säkerhetsåtgärder. Ansvaret för utförandet dessa säkerhetsåtgärder ligger hos respektive personuppgiftsansvariges nämnd. Åtgärderna vilka sammanfattas nedan skall uppfyllas innan en personuppgiftsansvarig nämnd eller bolag får påbörja behandling av känsliga personuppgifter i AI-plattformen.

1. **Avtalsmässig grund för behandling av känsliga personuppgifter**

Gällande huvudavtal (KS 2024/0609-11) med tillhörande PUB-avtal är ingångna med utgångspunkt från att kommunen inte skall använda känsliga personuppgifter. Behandlingen av känsliga personuppgifter innebär att avtalet behöver revideras. Innan behandling av känsliga personuppgifter inleds skall avtalsförhållandena granskas och vid behov antingen kompletteras eller ersättas med avtal som tydligt omfattar känsliga personuppgifter. Detta innefattar verifiering av samtliga underbiträden som anlitas för behandling av känsliga personuppgifter, vilka även skall redogöras i PUB-avtalets bilaga 2.

2. **Bekräftelse från personuppgiftsansvarig om avgränsning mot sekretess**

Den personuppgiftsansvariga nämnden eller bolaget som har för avsikt att inleda behandlingen skall skriftligen bekräfta för AI-administratören att den planerade behandlingen inte omfattar sekretess enligt offentlighets- och sekretesslagen. Bekräftelsen skall avse samtliga användarfall som planeras inom behandlingen och dokumenteras i den personuppgiftsansvariges behandlingsregister.

3. **Teknisk konfiguration av säkerhetsklassning**

AI-administratören skall, med stöd av AI-plattformens funktion för säkerhetsklassning (Security Classification), konfigurera tilldelningen av modeller, verktyg och kunskapssamlingar på ett sätt som innebär att varje personuppgiftsansvarig endast får tillgång till de delar av plattformen som motsvarar det scope som bekräftelsen från respektive personuppgiftsansvarige angivit enligt punkt 2 ovan.

4. **Fullföljd användarutbildning**

Samtliga användare som ges behörighet att behandla känsliga personuppgifter skall ha genomfört den av kommunens vid var tids fastställda utbildning. Utbildningen skall omfatta avgränsningen mot sekretessbelagda uppgifter, samt skyldigheten att avstå från att föra in sådana uppgifter i AI-plattformen.

5. **Uppdaterad handlingsplan kopplat till informationsklassning**

Informationssäkerhetssamordnare skall tillsammans med systemförvaltaren granska handlingsplanen och vid behov uppdatera densamma med kompletterande säkerhetsåtgärder som tillkommer på grund av att känsliga personuppgifter behandlas.

6. Information till de registrerade

Övergripande information om behandlingen i AI-plattformen skall finnas tillgänglig på kommunens hemsida innan driftsättning. Förvaltningsspecifik information skall publicera på respektive förvaltnings- och bolags hemsida.

7. Dokumenterat ställningstagande till artikel 9-undantag

Den personuppgiftsansvarige skall ha dokumenterat det undantag enligt artikel 9.2 GDPR jämte tillhörande nationell rätt som åberopas för respektive användarfall i sitt behandlingsregister.

9. Förankra bedömningen i organisationen

Konsekvensbedömningen ska förankras i organisationen för att säkerställa att de slutsatser och förhandsvillkor som dokumentet anger är kända, accepterade och praktiskt genomförbara hos de funktioner som ska tillämpa dem.
Förankringen sker i följande led:

Dataskyddsombudet (DSO) har granskat konsekvensbedömningen och avgett rekommendationer enligt avsnitt 7.1. DSO:s synpunkter har beaktats i den slutliga versionen av dokumentet, och avvikelser från DSO:s rekommendationer redovisas särskilt.

GDPR-samordnare och informationssäkerhetssamordnare på kommunstyrelsens förvaltning har medverkat i framtagandet av konsekvensbedömningen och ansvarar för att förhandsvillkoren i avsnitt 8 förmedlas till respektive personuppgiftsansvarig nämnd eller bolag inför aktivering av AI-plattformen.

Respektive personuppgiftsansvarig nämnd och bolag informeras om konsekvensbedömningens innehåll och de förhandsvillkor som åligger dem inför egen aktivering av plattformen. Förankringen sker genom GDPR-samordnaren och dokumenteras i respektive personuppgiftsansvariges behandlingsregister.

Kommunledningen informeras om konsekvensbedömningens slutsatser och de strukturella förutsättningar, särskilt AI-administratörens funktion och säkerhetsklassningen, som krävs för att behandlingen ska vara möjlig att genomföra.

Den av kommunstyrelsen utsedde AI-administratören tar del av konsekvensbedömningen i sin helhet eftersom funktionen är central för att förhandsvillkoren ska få praktisk verkan. Rutiner för funktionens utövande, dokumentation av aktiveringar och hantering av avvikelser fastställs inför driftsättning.

10. Följ upp konsekvensbedömningen kontinuerligt

Konsekvensbedömningen ska följas upp kontinuerligt för att säkerställa att förutsättningarna för bedömningen alltjämt är på plats och att de förhandsvillkor som föreskrivs i avsnitt 8 upprätthålls över tid.

Återkommande översyn

Konsekvensbedömningen ska ses över årligen samt vid väsentliga förändringar i behandlingen. Som väsentliga förändringar betraktas bland annat byte av leverantör eller underbiträden, ändringar i AI-plattformens funktionalitet som påverkar dataflöden eller säkerhetsklassning, lagstiftningsändringar som påverkar laglig grund eller tillämpliga undantag enligt artikel 9.2 GDPR, samt ny rättspraxis eller IMY-vägledning av betydelse för behandlingen.

Uppföljning av AI-administratörens funktion

Mot bakgrund av den strukturella observationen i avsnitt 5.2, att AI-administratörens funktion och säkerhetsklassningen tillsammans utgör grunden för riskreduceringen, ska funktionens upprätthållande särskilt följas upp. GDPR-samordnaren ska minst halvårsvis kontrollera att AI-administratören utför sin roll enligt fastställd rutin, att aktiveringar dokumenteras korrekt, att säkerhetsklassningen är konfigurerad i enlighet med respektive personuppgiftsansvariges bekräftelse, och att rutiner för vikariat och delegering är aktuella. Uppföljningen dokumenteras och rapporteras till informationssäkerhetssamordnaren.

Personoberoende och kontinuitet

Funktionen som AI-administratör ska vara dokumenterad och personoberoende. Rutiner för vikariat och delegering ska finnas i fastställd form. Vid byte av AI-administratör ska överlämning ske strukturerat och tidigare dokumentation av aktiveringar och konfigurationer överföras till efterträdaren.

Åtgärder vid avvikelse

Om det i efterhand framkommer, exempelvis i samband med uppföljning av regelefterlevnad, att personuppgiftsansvarig nämnd eller bolag behandlar personuppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen i AI-plattformen trots bekräftelsen om motsatsen enligt avsnitt 8, skall AI-administratören, utan dröjsmål temporärt återkalla tillgången för den berörda personuppgiftsansvarige.

En personuppgiftsincident enligt artikel 33 GDPR registreras och bedöms av den berörda personuppgiftsansvariges GDPR-samordnare i enlighet med kommunens instruktion för misstänkt personuppgiftsincident. Vid bedömt allvar ska dataskyddsombudet informeras.

Återupptagande av behandling efter återkallad tillgång kräver förnyad bekräftelse enligt avsnitt 8 samt, beroende på avvikelsens art, en kompletterande DPIA.

Per Eriksson

dataskyddsstrateg
kommunstyrelsens förvaltning

Bilagor
bilaga 1 - processkartläggning.xlsx
bilaga 2 - handlingsplan.xlsx
bilaga 3 - riskanalys.xlsx
bilaga 4 - rapport ai-användande.xlsx
bilaga 5 - Sekretessfrågan i Intrics AI-plattform. Utredningsbehov och fortsatt arbete.
bilaga 6 - Dataskyddsombudets yttrande
bilaga 7 - Bemötande av dataskyddsombudets yttrande

VARBERGS KOMMUN

Telefon: Varberg direkt: 0340-880 00. E-post: varbergdirekt@varberg.se. Webbplats: varberg.se Postadress: Varbergs kommun, 432 80 Varberg. Besöksadress: Varberg