Konsekvensbedömning - Intric AI-plattform

Lidköpings kommun

Motsvarar Steg 3–10 i En praktisk guide

Innehåll

Övergripande information 3
Steg 3. Systematisk beskrivning av personuppgiftsbehandlingen 4
3.1 Behandlingens art 4
3.2 Behandlingens omfattning 6
3.3 Behandlingens sammanhang 8
3.4 Behandlingens ändamål 10
3.5 Nödvändiga resurser 15
3.6 Funktionell beskrivning av behandlingen 18
3.7 Roller och ansvarsfördelning 24
Steg 4. Rättslig analys 30
4.1 Gällande regelverk 30
AI-förordningen (EU) 2024/1689 33
4.2 Dataskyddsprinciperna och den rättsliga grunden för behandlingen 33
4.3 Registrerades rättigheter 49
Praktiska begränsningar (förtydligande efter DSO:s yttrande) 53
4.4 Skyddsåtgärder för internationella överföringar 54
Transfer Impact Assessment (TIA) 61
4.5 Sammantagen bedömning 61
Steg 5. Riskhantering 63
Förtydligande av risker tillagda efter DSO:s yttrande 68
Steg 6. Bedömning av skyldigheten att begära förhandssamråd 68
Steg 7. Synpunkter som hämtats in från berörda 70
7.1 Dataskyddsombudets rekommendationer 70
7.2 Synpunkter från de registrerade 70
7.3 Synpunkter från övriga intressenter 72
Steg 8. Sammantagen bedömning 73
Steg 9. Förankring av bedömningen i organisationen 76
Steg 10. Kontinuerlig översyn 79
Bilagor 85

Övergripande information

Personuppgiftsansvarig för behandlingen

- **Organisation (inkl. organisationsnummer):** Lidköpings kommun 212000-1694
- **Adress:** Skaragatan 8, 531 32 Lidköping
- **Telefon:** 0510-77 00 00
- **E-post:** kommunstyrelsen@lidkoping.se

Kontaktuppgifter till dataskyddsombud

- **Organisationens dataskyddsombud:** Frida Sjökvist
- **Telefon:** 0510-771000
- **E-post:** dso@lidkoping.se

Ansvariga för konsekvensbedömningen

- **Ansvarig för att genomföra konsekvensbedömningen:**

  Inledningsvis genomförs konsekvensbedömningen inom kommunstyrelsens (personuppgiftsansvarig) organisation, av enheten Verksamhetsutveckling och digitalisering. Enheten beskriver systemet övergripande, identifierar tillämplig laglig grund samt bedömer generella och gemensamma risker kopplade till personuppgiftsbehandlingar i systemet. Detta utgör ett gemensamt underlag som respektive personuppgiftsansvarig inom kommunen kan utgå från — och vid behov komplettera med verksamhetsspecifika risker och besluta om ytterligare åtgärder.

- **Ansvarig för innehållet i denna konsekvensbedömningen och de bedömningar som görs:** Chef verksamhetsutveckling och digitalisering.

- **Roller som deltagit i arbetet med att genomföra konsekvensbedömningen:**

  Systemförvaltare Intric, informationssäkerhetssamordnare, utvecklingsledare från enhet för verksamhetsutveckling och digitalisering, DSO, IT-säkerhetsspecialister.

- **Ansvarig för att hantera eventuella kvarvarande risker efter att konsekvensbedömningen avslutats:** Chef verksamhetsutveckling och digitalisering.

- **Ansvarig för att följa upp konsekvensbedömningen:** Chef verksamhetsutveckling och digitalisering.

Steg 3. Systematisk beskrivning av personuppgiftsbehandlingen

3.1 Behandlingens art

Allmän beskrivning och bakgrund

Lidköpings kommun planerar att införa AI-plattformen Intric som ett arbetsverktyg för kommunens medarbetare. Plattformen ska ge personalen tillgång till olika språkmodeller (stora språkmodeller, LLM) för att effektivisera och förbättra kvaliteten i textproduktion, administration och analys inom ramen för kommunens verksamhet.

Intric är en AI-assistent-plattform som möjliggör för användare att interagera med olika språkmodeller genom en säker och kontrollerad miljö. Plattformen erbjuder flera driftsalternativ och modellval, där kommunen har valt en dedikerad instans i cloud-miljö med fokus på dataskydd och kontroll.

Bakgrund till införandet:

Den snabba utvecklingen inom AI-teknik och språkmodeller har skapat nya möjligheter för offentlig sektor att effektivisera sitt arbete och höja kvaliteten i kommunikationen med invånare. Samtidigt ställer användningen av dessa verktyg höga krav på dataskydd, informationssäkerhet och ansvarsfull användning.

Lidköpings kommun har identifierat ett behov av att ge medarbetare tillgång till AI-stöd för en rad specifika arbetsuppgifter, samtidigt som personuppgifter och annan känslig information skyddas. Genom att införa en kontrollerad plattform med tydliga riktlinjer och tekniska skyddsåtgärder kan kommunen realisera fördelarna med AI-teknik samtidigt som riskerna minimeras.

Omfattning av behandlingen:

Denna konsekvensbedömning omfattar användningen av Intric-plattformen för kommunens medarbetare, där personuppgifter behandlas enligt följande:

1. **Plattformsadministration:** Intric-plattformen hanterar grundläggande identitetsuppgifter om upp till cirka 4 000 användare (kommunens medarbetare) bestående av namn, efternamn och e-postadress. Dessa uppgifter används för autentisering, åtkomststyrning och administration av användarkonton.
2. **Användning av språkmodeller:** Användare kan interagera med olika språkmodeller genom plattformen för att utföra specificerade arbetsuppgifter. Vid denna användning kan personuppgifter om externa personer (inte kommunens medarbetare) förekomma i prompter och bifogade filer, begränsat till namn, efternamn, e-postadress, LinkedIn-profil och telefonnummer.
3. **Strikta begränsningar:** Behandlingen omfattar INTE känsliga personuppgifter enligt artikel 9 GDPR eller uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen. Kommunen har etablerat tydliga riktlinjer och tekniska åtgärder i form av användarvarningar (UX) för att förhindra att sådan information hanteras i plattformen.

Teknisk lösning:

Kommunen har valt driftsalternativet "Dedikerad instans Cloud" vilket innebär att varje tenant (Lidköpings kommun) har en isolerad databas på en gemensam server hos underleverantören Glesys AB i Sverige.

Språkmodeller som används:

Följande språkmodeller kommer att vara tillgängliga för användare:

1. **Managed by Intric (Swedish Hosted)** - Open Source-modell som hostas och driftas av Intric själva via Airon i Sverige. Denna modell baseras initialt på OpenAI:s gpt-oss men kommer löpande att bytas ut när bättre Open Source-modeller som kan driftas på samma sätt finns tillgängliga.
2. **Llama 3.3 SWE (Meta)** - Open Source-modell från Meta, hostad i Sverige via Intric/Airon.
3. **Mistral** - Modeller från Mistral AI (franskt företag, behandling inom EU).
4. **OpenAI GPT-modeller** - Proprietära modeller från OpenAI (amerikanskt företag, behandling i USA).
5. **Claude (Anthropic)** - Proprietära modeller från Anthropic (amerikanskt företag, behandling i USA).

Privacy by design - Kommunstyrelsens rekommendation:

I enlighet med principen om inbyggt dataskydd (privacy by design, artikel 25 GDPR) rekommenderar kommunen användning av **Managed by Intric (Swedish Hosted), Llama 3.3 SWE eller Mistral** som förstahandsval för arbetsuppgifter som kan innehålla personuppgifter. Dessa modeller erbjuder behandling inom Sverige eller EU/EES och ger därmed högre kontroll och lägre risk för tredjelandsöverföringar.

Användare har dock frihet att välja andra tillgängliga modeller, såsom OpenAI och Anthropic, baserat på sina specifika behov, under förutsättning att respektive sektors systemadministratörer har tillgängliggjort dessa. Användningen ska ske i enlighet med kommunens riktlinjer och med medvetenhet om att dessa alternativ innebär överföring av data till USA (se avsnitt 4.4 för bedömning av skyddsåtgärder).

För modeller som driftas av externa aktörer (OpenAI, Anthropic) sker kommunikationen via krypterade anrop och endast följande information delas med dessa underleverantörer:

- Kontexten (information som användaren skriver i chatten eller laddar upp)
- IP-adressen från där Intric-applikationen driftas (inte användarens IP-adress)

Ingen annan information om användaren (som namn, e-post eller användar-ID) delas med AI-modelleverantörerna.

Personuppgiftsbiträdesavtal:

Kommunen har tecknat personuppgiftsbiträdesavtal med Intric AB som reglerar ansvarsfördelning, säkerhetsåtgärder och villkor för behandlingen av personuppgifter.

Kategorier av personuppgifter

Nr	Kategori av personuppgifter	Särskild kategori av personuppgifter
01	Namn på kommunens medarbetare (för- och efternamn)	Nej
02	E-postadresser till kommunens medarbetare	Nej
03	Användar-ID i Intric-plattformen	Nej
04	Tekniska loggdata (tidsstämplar, aktivitetsloggar) kopplade till användarkonton	Nej
05	Namn på externa personer som kan förekomma i användarens prompter och filer	Nej
06	E-postadresser till externa personer som kan förekomma i användarens prompter och filer	Nej
07	Telefonnummer till externa personer som kan förekomma i användarens prompter och filer	Nej
08	LinkedIn-profiler för externa personer som kan förekomma i användarens prompter och filer	Nej

Kategorier av registrerade

Nr	Kategori av registrerade	Särskild kategori av registrerade
01	Kommunens anställda medarbetare	Beroendeställning (anställningsförhållande)
02	Externa kontaktpersoner (t.ex. konsulter, tjänstepersoner från andra organisationer)	Nej

3.2 Behandlingens omfattning

Behandlingens volym

Den behandling som avses omfattar personuppgifter om cirka **4 000 medarbetare** inom Lidköpings kommun. Detta motsvarar det maximala antalet användarkonton som kan skapas i Intric-plattformen.

För varje användare behandlas:

- För- och efternamn
- E-postadress
- Användar-ID
- Loggdata kopplat till användarkontot

Detta innebär ungefär 4 kategorier av personuppgifter per användare avseende själva plattformsadministrationen.

Personuppgifter i användarinteraktion:

Utöver de grundläggande användaruppgifterna kan personuppgifter om externa personer förekomma när medarbetare använder språkmodellerna. Baserat på de tydligt definierade ändamålen, vilka anges i den här konsekvensbedömningen, samt restriktionerna mot känsliga uppgifter bedöms omfattningen dock vara begränsad och kopplad till:

- Namn och kontaktuppgifter till externa samarbetspartners i kommunikation och textproduktion
- Namn i dokumentation och administrativa texter
- Namn och roller i projektdokumentation och rapporter

Frekvens av insamling:

Personuppgifter om medarbetare som behandlas vid:

- Skapande av användarkonto i plattformen (engångsvis per användare)
- Uppdatering av användaruppgifter vid behov (sporadiskt)
- Kontinuerlig loggning av användaraktivitet under tiden användaren är aktiv i plattformen

Personuppgifter om externa personer samlas inte in av plattformen aktivt, utan förekommer endast om användare själva väljer att inkludera sådana i sina prompter eller bifogade filer.

Den totala mängden personuppgifter uppskattas till:

- Cirka 16 000 dataposter för användaradministration (4 000 användare × 4 uppgiftskategorier)
- Loggdata som genereras löpande baserat på användning
- Varierande mängd personuppgifter om externa personer i användarinteraktioner, vars omfattning beror på faktisk användning

Behandlingens geografiska omfattning

Primär datalagring:

Personuppgifter som behandlas i Intric-plattformen lagras hos underleverantören **Glesys AB**. Glesys AB är en svensk leverantör som driver datacenter i Sverige. All lagring av användardata, databaser och säkerhetskopior sker på virtuella KVM- och VMware-servrar hos Glesys i Sverige.

Behandling via språkmodeller:

Beroende på vilken språkmodell användaren väljer kan personuppgifter behandlas i olika geografiska områden:

1. **Managed by Intric (Swedish Hosted):** Behandling sker i **Sverige** via Airons infrastruktur. Detta är en Open Source-modell som hostas lokalt.
2. **Llama 3.3 SWE (Meta):** Behandling sker i **Sverige** via Airons infrastruktur. Open Source-modell hostad lokalt.
3. **Mistral:** Mistral AI är ett franskt företag. Vid användning av dessa modeller sker behandling inom **EU/EES** (Frankrike).
4. **OpenAI GPT-modeller:** OpenAI är ett amerikanskt företag. Vid användning av dessa modeller överförs kontexten (prompter och bifogade filer) till **USA**.
5. **Claude (Anthropic):** Anthropic är ett amerikanskt företag. Vid användning av dessa modeller överförs kontexten till **USA**.

Skyddsåtgärder för internationella överföringar:

För de amerikanska leverantörerna (OpenAI och Anthropic) gäller särskilda skyddsåtgärder. Se **avsnitt 4.4** för fullständig genomgång av tredjelandsöverföringar och skyddsåtgärder.

Användarhantering:

Användarhantering (autentisering och åtkomststyrning) sköts via Glesys server i Sverige.

Sammanfattning geografisk omfattning:

- **Primär datalagring:** Sverige (Glesys AB)
- **Användarhantering:** Sverige (Glesys AB)
- **AI-behandling:** Beroende på vald modell – Sverige (Managed by Intric, Llama 3.3 SWE), EU (Mistral) eller USA (OpenAI, Anthropic)

3.3 Behandlingens sammanhang

Behandlingen av personuppgifter inom Intric-plattformen sker i ett kommunalt sammanhang där medarbetare utför sina arbetsuppgifter inom olika verksamhetsområden. Kommunen har ett ansvar att leverera kvalitativ service till invånare samtidigt som den hanterar offentlig information på ett säkert och rättssäkert sätt.

Interna faktorer:

Lidköpings kommun har identifierat ett behov av att modernisera sina arbetssätt och dra nytta av AI-teknik för att förbättra effektiviteten och kvaliteten i kommunikationen. Samtidigt är kommunen väl medveten om de särskilda krav som ställs på offentlig sektor vad gäller informationssäkerhet, dataskydd och transparens.

Kommunen har begränsad tidigare erfarenhet av att använda externa AI-tjänster i verksamheten. Införandet av Intric utgör därför en delvis innovativ satsning som kräver noggrann planering, utbildning och uppföljning.

Externa faktorer:

AI-teknik och språkmodeller har utvecklats snabbt under senare år och används alltmer i både privat och offentlig sektor. Samtidigt har denna utveckling medfört ökad uppmärksamhet kring risker för dataskydd, integritet och missbruk. Användningen av amerikanska AI-tjänster har särskilt uppmärksammats med avseende på tredjelandsöverföringar och risker för myndigheters åtkomst enligt amerikansk lagstiftning (t.ex. CLOUD Act).

Integritetsskyddsmyndigheten (IMY) och Europeiska dataskyddsstyrelsen (EDPB) har utfärdat vägledning om användning av AI-system och behandling av personuppgifter i sådana sammanhang.

Registrerades kontroll och förväntningar:

Medarbetare i kommunen som får tillgång till Intric har begränsad kontroll över hur deras grundläggande användaruppgifter (namn, e-post) behandlas i plattformen, eftersom detta är nödvändigt för att få tillgång till systemet. De har dock full kontroll över vilken information de själva väljer att dela med AI-modellerna genom sina prompter och bifogade filer.

Externa personer vars personuppgifter kan förekomma i användarinteraktioner (t.ex. namn i en projektplan eller kontaktuppgifter i en kommunikationsmall) har ingen direkt kontroll över behandlingen och är sannolikt omedvetna om att deras uppgifter kan komma att behandlas i en AI-plattform.

Beroendeförhållanden:

Kommunens medarbetare befinner sig i ett beroendeförhållande gentemot arbetsgivaren. Användning av Intric är dock inte obligatorisk utan utgör ett frivilligt verktyg som medarbetare kan välja att använda för vissa arbetsuppgifter. Det finns alternativa metoder för att utföra samma arbetsuppgifter utan att använda AI-stöd.

Relation till uppförandekoder och certifieringar:

Intric AB har certifieringar enligt **ISO/IEC 27001:2022** (informationssäkerhet). Underleverantören Glesys AB driver datacenter med hög säkerhetsstandard i Sverige. Intric uppfyller **informationssäkerhetskrav 3-3-3** för konfidentialitet, riktighet och tillgänglighet.

För de externa AI-modellerna (OpenAI, Anthropic, Mistral, Meta) finns olika certifieringar och säkerhetsramverk som dessa företag följer, men Lidköpings kommun har begränsad insyn i och kontroll över dessa leverantörers interna processer och säkerhetsåtgärder.

Innovationsaspekten:

Användningen av AI-verktyg i kommunal verksamhet är relativt ny och innebär att nya arbetsmetoder införs. Detta kan upplevas som innovativt av både medarbetare och externa intressenter. Kommunen är medveten om att användningen av AI-verktyg kan väcka frågor och oro hos invånare och andra intressenter, särskilt vad gäller dataskydd och transparens.

Tidigare erfarenheter:

Kommunen har begränsad tidigare erfarenhet av att använda molnbaserade AI-tjänster med externa leverantörer i stor skala. Det finns därför ett behov av att noggrant följa upp användningen, identifiera eventuella problem och säkerställa att de fastställda riktlinjerna följs i praktiken.

Uppföljning och kontroll:

Intric-plattformen erbjuder loggning och spårbarhet av användaraktivitet, vilket ger kommunen möjlighet att följa upp hur systemet används och upptäcka eventuella avvikelser från fastställda riktlinjer. Denna möjlighet till uppföljning är en viktig faktor för att säkerställa ansvarsfull användning.

Sammanfattning av sammanhanget:

Behandlingen sker i ett sammanhang där kommunen som offentlig aktör har höga krav på sig att skydda personuppgifter och agera transparent. Införandet av AI-teknik är delvis innovativt och kräver noggrann planering, tydliga riktlinjer och kontinuerlig uppföljning för att säkerställa att riskerna hanteras på ett adekvat sätt. Beroendeförhållandet mellan kommunen och dess medarbetare samt den begränsade kontrollen för externa personer vars uppgifter kan förekomma i interaktioner kräver särskild uppmärksamhet.

3.4 Behandlingens ändamål

Ändamålet med personuppgiftsbehandlingen i Intric-plattformen är att tillhandahålla kommunens medarbetare ett säkert och kontrollerat AI-verktyg för att effektivisera och förbättra kvaliteten i specifika arbetsuppgifter som inte involverar känsliga personuppgifter eller sekretessbelagd information.

Behandlingen omfattar två huvudsakliga komponenter:

1. Användaradministration i plattformen

För att medarbetare ska kunna använda Intric-plattformen måste deras identitet verifieras och de måste ges behörighet till systemet. Detta kräver behandling av grundläggande identitetsuppgifter (namn, e-postadress, användar-ID) och loggning av användaraktivitet.

Specifika ändamål för användaradministration:

- Autentisering och åtkomststyrning för att säkerställa att endast behöriga medarbetare kan använda plattformen
- Administration av användarkonton
- Säkerställande av spårbarhet och möjlighet att utreda eventuella incidenter eller avvikelser genom loggning
- Uppföljning av systemanvändning för att kunna utvärdera nyttan och identifiera förbättringsområden

2. Användning av AI-språkmodeller för specificerade arbetsuppgifter

Medarbetare ska kunna använda AI-språkmodeller genom plattformen för att få stöd i sitt arbete inom tydligt avgränsade ändamål. Dessa ändamål är specifikt utformade för att endast omfatta arbetsuppgifter där det inte förekommer känsliga personuppgifter eller sekretessbelagd information.

Specificerade ändamål per verksamhetsområde:

A) Kommunikation och textproduktion

Specifikt ändamål: Effektivisera framtagning av texter och förbättra språklig kvalitet och tillgänglighet i kommunikation med invånare och externa parter om offentliga ärenden.

Konkreta användningsfall (utan känsliga uppgifter eller sekretess):

- Skapa första utkast till informationsbrev om nya rutiner, öppettider och verksamhetsförändringar
- Omskriva offentlig information från webbplatser till enklare och mer tillgängligt språk enligt klarspråksprinciper
- Utveckla standardmallar för allmän e-postkommunikation
- Sammanfatta offentliga mötesprotokoll som inte omfattas av sekretess
- Skapa utkast till nyhetsartiklar om invigningar, nya tjänster och verksamhetsinformation
- Översättningsstöd för förenkling av komplexa offentliga texter till lättläst svenska
- Framtagning av innehåll för sociala medier om kommunala aktiviteter
- Utveckla informationsblad och broschyrer om kommunala tjänster

Personuppgifter som kan förekomma: Namn på kommunala representanter, kontaktpersoner, e-postadresser till offentliga funktioner.

B) Administration och intern effektivisering

Specifikt ändamål: Minska manuell textproduktion, förbättra struktur och dokumentation för att öka administrativ effektivitet i icke-sekretessbelagda processer.

Konkreta användningsfall:

- Utveckla rutin- och processbeskrivningar för attestrutiner och administrativa flöden
- Skapa checklistor för olika verksamhetsområden (ej personrelaterade)
- Strukturera rapportmallar för verksamhetsrapporter och utvärderingar
- Förbättra befintliga dokument genom omstrukturering
- Sammanfatta offentliga rapporter och årsredovisningar
- Utveckla projektdokumentation
- Skapa manualer och användarguider

Personuppgifter som kan förekomma: Namn på projektdeltagare, ansvariga för processer, kontaktpersoner.

C) Kompetensutveckling och lärande

Specifikt ändamål: Underlätta lärande, reflektion och kunskapsspridning för att höja kompetensen i organisationen.

Konkreta användningsfall:

- Skapa interaktiva övningar och quiz för utbildningar

- Förklara komplexa begrepp och regelverk
- Utveckla reflektionsfrågor för utbildningar
- Skapa kursmaterial och introduktioner
- Förenkla styrdokument
- Utveckla presentationsmaterial

Personuppgifter som kan förekomma: Namn på kursledare, föreläsare, författare.

D) Analys och beslutsstöd

Specifikt ändamål: Förbättra analys av offentlig verksamhetsdata för att stödja evidensbaserat beslutsfattande.

Konkreta användningsfall:

- Sammanställning av avidentifierade enkätsvar
- Utveckla riskmatriser för nya e-tjänster
- Genomföra SWOT-analyser för digitaliseringsstrategier
- Föreslå relevanta nyckeltal för verksamhetsmätning
- Utveckla rapportstrukturer
- Benchmarking och trendanalyser

Personuppgifter som kan förekomma: Namn på verksamhetsansvariga, kontaktpersoner vid andra kommuner.

E) Invånardialog och samhällsinformation

Specifikt ändamål: Stärka tillgänglig kommunikation och transparens för att förbättra demokratisk delaktighet och service.

Konkreta användningsfall:

- Skapa instruktioner för e-tjänster
- Utveckla enkätfrågor för invånardialoger
- Utforma texter till informationsskyltar
- Skapa pressmeddelanden
- Översätta kommunala beslut till enkelt språk
- Utveckla FAQ-dokument
- Skapa sammanfattningar av budgetar och styrdokument

Personuppgifter som kan förekomma: Namn på beslutsfattare, kontaktpersoner, pressansvariga.

F) IT, digitalisering och innovation

Specifikt ändamål: Stöd för teknisk utveckling, kravställning och automatisering för att accelerera digitaliseringsarbetet.

Konkreta användningsfall:

- Generera fiktiva testdata för systemtester
- Kodskrivning för skript och konfigurationer
- Förklara tekniska skillnader mellan system
- Utveckla kravspecifikationer
- Beskriva IT-supportprocesser
- Skapa API-dokumentation och tekniska beskrivningar
- Utveckla IT-säkerhetsriktlinjer

Personuppgifter som kan förekomma: Namn på IT-ansvariga, systemägare, leverantörskontakter.

G) Projektplanering och genomförande

Specifikt ändamål: Förbättra planering, dokumentation och uppföljning av offentliga projekt.

Konkreta användningsfall:

- Utveckla projektplaner
- Skapa statusrapporter
- Identifiera projektrisker
- Skapa standardiserade projektdokument
- Utveckla slutrapporter

Personuppgifter som kan förekomma: Namn på projektdeltagare, projektledare, styrgruppsledamöter, externa samarbetspartners.

H) Kvalitet och verksamhetsuppföljning

Specifikt ändamål: Förbättra uppföljning och kvalitetssäkring av offentlig verksamhet.

Konkreta användningsfall:

- Definiera mätbara kvalitetsmått
- Skapa mallar för verksamhetsuppföljning
- Analysera verksamhetsdata för förbättringsområden
- Utveckla metoder för att mäta invånartillfredsställelse
- Genomföra benchmarking-analyser

Personuppgifter som kan förekomma: Namn på verksamhetsansvariga, kvalitetssamordnare.

I) Teknisk support och användarstöd

Specifikt ändamål: Förbättra support och hjälpfunktioner för medarbetare och invånare.

Konkreta användningsfall:

- Utveckla felsökningsguider
- Skapa användarmanual och guider
- Utveckla FAQ-dokument
- Skapa standardsvar för supportärenden
- Utveckla instruktionsmaterial
- Skapa beslutsträd och troubleshooting-flöden

Personuppgifter som kan förekomma: Namn på IT-supportpersonal, systemansvariga.

J) Övriga specificerade ändamål

Ytterligare verksamhetsområden där AI-stöd kan användas för offentliga, icke-sekretessbelagda arbetsuppgifter:

- Ekonomisk administration
- Fastighets- och markförvaltning
- Miljö och samhällsplanering
- Juridik och styrning
- Forskning och utveckling

Personuppgifter som kan förekomma: Namn och kontaktuppgifter till ansvariga tjänstepersoner, externa samarbetspartners, konsulter och leverantörer.

Avgränsningar - vad som INTE omfattas

Följande ändamål och användningsområden omfattas **INTE** av denna behandling och får **INTE** hanteras i Intric-plattformen:

- Hantering av säkerhetsskyddsklassificerade uppgifter, ärenden eller information som omfattas av sekretess enligt offentlighets- och sekretesslagen
- Behandling av känsliga personuppgifter enligt artikel 9 GDPR (t.ex. hälsouppgifter, uppgifter om etniskt ursprung, religiös övertygelse)
- Individrelaterad dokumentation inom social omsorg, vård, skola eller annan verksamhet där känsliga uppgifter förekommer
- Beslut eller handläggning som involverar enskildas rättsliga ställning
- Personalärenden som involverar enskilda medarbetares personliga förhållanden
- Behandling av uppgifter om underåriga barn
- Brottsutredningar

Nödvändighet och proportionalitet

Behandlingen är **nödvändig** för att möjliggöra för kommunens medarbetare att använda moderna AI-verktyg för att effektivisera sitt arbete och höja kvaliteten i kommunikation och service till invånare. De specificerade ändamålen är noga avgränsade till områden där det inte förekommer känsliga personuppgifter eller sekretessbelagd information.

Behandlingen är **proportionerlig** i förhållande till ändamålen eftersom:

- Endast grundläggande identitetsuppgifter om medarbetare behandlas för plattformsadministration
- Personuppgifter om externa personer som kan förekomma i användarinteraktioner är begränsade till grundläggande kontaktuppgifter
- Tydliga riktlinjer och tekniska varningar i användargränssnittet förhindrar att känsliga uppgifter eller sekretess hanteras
- Alternativa metoder (manuell textproduktion, externa konsulter) skulle vara betydligt mer kostsamma och tidskrävande utan att uppnå samma kvalitet och tillgänglighet

3.5 Nödvändiga resurser

För att kunna genomföra den planerade personuppgiftsbehandlingen i Intric-plattformen krävs följande resurser och informationstillgångar:

1. Infrastruktur och servermiljö

Intric-plattformen:

- Molnbaserad plattform för AI-assistenter tillhandahållen av Intric AB
- Driftsalternativ: Dedikerad instans Cloud hos underleverantören Glesys AB
- Webbserver och applikationsserver för att hantera användarförfrågningar och kommunikation

Databas:

- Dedikerad databas på gemensam server hos Glesys AB i Sverige
- Används för lagring av användaruppgifter, loggdata och konfigurationsinformation
- Isolerad från andra tenanter för att säkerställa dataseparation

Användarhantering:

- Serverinfrastruktur hos Glesys för hantering av autentisering och åtkomstkontroll
- Integration med kommunens identitetshanteringssystem (om tillämpligt)

2. AI-modeller och externa tjänster

Språkmodeller:

Följande AI-modeller kommer att vara tillgängliga för användare:

A) Managed by Intric (Swedish Hosted) *(Rekommenderad)*

- Open Source-modell som hostas och driftas av Intric via Airon i Sverige
- Baserad initialt på OpenAI:s gpt-oss, kommer bytas ut löpande
- Lokal hosting i Sverige ger hög datakontroll
- **Rekommenderas enligt privacy by design-principen**

B) Llama 3.3 SWE (Meta) *(Rekommenderad)*

- Open Source-modell från Meta
- Hostad i Sverige via Intric/Airon
- Specialiserad för svenska språket
- **Rekommenderas enligt privacy by design-principen**

C) Mistral *(Rekommenderad)*

- Modeller från Mistral AI (franskt företag)
- Behandling inom EU/EES
- **Rekommenderas enligt privacy by design-principen**

D) OpenAI GPT-modeller

- Proprietära modeller från OpenAI (amerikanskt företag)
- Behandling sker i USA
- *Användare väljer aktivt denna modell och är informerade om tredjelandsöverföring (se avsnitt 4.4)*

E) Claude (Anthropic)

- Proprietära modeller från Anthropic (amerikanskt företag)
- Behandling sker i USA
- *Användare väljer aktivt denna modell och är informerade om tredjelandsöverföring (se avsnitt 4.4)*

3. Säkerhets- och skyddsåtgärder

Kryptering och säker kommunikation:

- SSL/TLS-kryptering för all kommunikation mellan användare och plattform
- Kryptering mellan Intricswebbserver och applikationsserver
- Krypterade anrop till externa AI-modelleverantörer

Autentisering och åtkomstkontroll:

- Inloggningssystem för att verifiera användaridentitet (SSO med BankID)

- Rollbaserad åtkomstkontroll för att styra åtkomst
- Multifaktorautentisering via BankID

Loggning och spårbarhet:

- Loggningsfunktioner för att registrera användaraktivitet
- Tidsstämplar och användar-ID kopplade till händelser
- Lagring av loggdata för säkerhetsövervakning och incidenthantering
- SIEM-system för centraliserad logghantering

4. Användarenheter och nätverk

Användarenheter:

- Datorer, surfplattor eller andra enheter som medarbetare använder för att komma åt Intric-plattformen
- Webbläsare med stöd för moderna webbstandarder
- Internetanslutning för att kommunicera med molnbaserade tjänster

Nätverksinfrastruktur:

- Kommunens nätverk och internetanslutning för att möjliggöra åtkomst till Intric-plattformen
- Eventuell VPN eller annan säker anslutning om åtkomst sker från externa nätverk

5. Avtal och dokumentation

Personuppgiftsbiträdesavtal (PUB-avtal):

- PUB-avtal mellan Lidköpings kommun och Intric AB som reglerar ansvarsfördelning och säkerhetsåtgärder
- Underbiträdesavtal mellan Intric och deras underleverantörer (Glesys, Airon, AI-modelleverantörer)

Riktlinjer och instruktioner:

- Kommunens riktlinjer för användning av Intric-plattformen (Riktlinjer för artificiell intelligens (AI) – Lidköpings kommunkoncern)
- Instruktioner för vilka typer av information som får och inte får hanteras
- Utbildningsmaterial för medarbetare

Påminnelser och information i plattformen:

- Informationstexter och påminnelser i Intric-plattformen som informerar användare om att inte dela känsliga uppgifter eller sekretessbelagd information
- Tydlig märkning av vilka typer av uppgifter som inte får behandlas

- Information om vilka modeller som behandlar data i Sverige/EU respektive USA

OBS: Det finns ingen automatisk scanning som detekterar och blockerar känsligt innehåll. Skyddet bygger på användarens ansvar, utbildning och kommunens riktlinjer.

6. Kompletterande system

Integration med kommunens IT-miljö:

- Integration med kommunens Active Directory för automatisk provisionering av användarkonton.

7. Support och förvaltning

Support från Intric AB:

- Teknisk support och underhåll av plattformen
- Uppdateringar och patchning av säkerhetsproblem
- Övervakning av systemets tillgänglighet och prestanda

Intern support:

- Systemadministratör per sektor (hanterar konton och behörigheter)
- Funktionsansvarig (stödjer användare av assistenter)
- Systemförvaltare (daglig drift, utbildning)
- Leverantör (teknisk drift, teknisk felsökning, säkerhet)

Sammanfattning:

För att genomföra behandlingen krävs en komplex infrastruktur bestående av molnbaserade servrar, databaser, AI-modeller från olika leverantörer, säkerhetsåtgärder som kryptering och loggning, samt användarenheter och nätverk. Avtal och riktlinjer utgör viktiga resurser för att säkerställa att behandlingen sker på ett rättssäkert och säkert sätt. Kombinationen av tekniska och organisatoriska åtgärder skapar förutsättningar för en kontrollerad och ansvarsfull användning av AI-tekniken.

3.6 Funktionell beskrivning av behandlingen

Denna beskrivning redogör för hur personuppgiftsbehandlingen i Intric-plattformen går till i praktiken, från att en användare skapar ett konto till att personuppgifter raderas.

Fas 1: Onboarding och skapande av användarkonton

Steg 1: Identifiering av behöriga användare

Verksamhetschefer identifierar vilka medarbetare som ska ges tillgång till Intric-plattformen. Behörighet baseras på arbetsroll och arbetsuppgifter.

Steg 2: Insamling av grundläggande uppgifter

För varje medarbetare som ska få tillgång samlas följande uppgifter in från kommunens befintliga system (t.ex. HR-system eller Active Directory):

- För- och efternamn
- E-postadress (arbetsmail)

Dessa uppgifter hämtas från intern källa inom kommunens IT-miljö och delas med Intric AB för att skapa användarkonton.

Steg 3: Skapande av användarkonto

Intric AB skapar användarkonton baserat på de mottagna uppgifterna. Varje användare tilldelas:

- Ett unikt användar-ID i Intric-plattformen
- Inloggningsuppgifter (SSO med BankID)

Användaruppgifterna lagras i Intricsderivkerade databas hos Glesys AB i Sverige.

Fas 2: Användning av plattformen

Steg 5: Inloggning och autentisering

Användaren loggar in på Intric-plattformen via webbläsare:

1. Användaren loggar in med SSO och sitt BankID
2. Inloggningsförfrågan skickas krypterat (SSL/TLS) till Intricswebbserver hos Glesys
3. Intricsautentiseringssystem verifierar användarens identitet mot databasen
4. Vid godkänd autentisering ges användaren åtkomst till plattformen

Loggning: Vid inloggning registreras tidsstämpel och användar-ID i loggfiler för säkerhetsövervakning.

Steg 6: Val av språkmodell och AI-assistent

Användaren ser bara de assistenter som de har behörigheter för. Det framgår där tydligt:

- Vad assistenten kan användas till och hur den ej får användas
- Vilka modeller som rekommenderas (svenska/EU-baserade)
- Vilka modeller som innebär överföring till USA

Steg 7: Interaktion med AI-modellen

Användaren skriver en prompt (fråga eller instruktion) och kan välja att bifoga filer.

Information och påminnelser: Användare informeras genom tydlig UX-design att:

- Känsliga personuppgifter inte får anges
- Sekretessbelagd information inte får delas
- Endast information som är offentlig eller icke-känslig får behandlas

- Svenska/EU-baserade modeller rekommenderas för personuppgifter

OBS: Det finns ingen automatisk scanning eller teknisk kontroll som förhindrar att känsligt innehåll skickas. Ansvaret ligger på användaren att följa kommunens riktlinjer.

Steg 8: Behandling av prompten

När användaren skickar sin prompt händer följande:

A) Kommunikation till AI-modellen

Prompten och eventuellt bifogade filer skickas från Intricsapplikationsserver till den valda AI-modelleverantören via krypterad anslutning (SSL/TLS).

Information som delas med AI-modelleverantören:

- Kontexten (själva prompten och bifogade filer)
- IP-adressen från Intricsserver (INTE användarens IP-adress)

Information som INTE delas:

- Användarens namn
- Användarens e-postadress
- Användar-ID

B) Behandling hos AI-modelleverantören

AI-modellen bearbetar prompten och genererar ett svar. Behandlingen sker i enlighet med respektive leverantörs villkor och dataskyddspolicy:

- **För Managed by Intric och Llama 3.3 SWE:** Behandling i Sverige via Airon
- **För Mistral:** Behandling inom EU (Frankrike)
- **För OpenAI och Anthropic:** Behandling i USA (se avsnitt 4.4 för skyddsåtgärder)

Datalagring hos AI-modelleverantörer:

Enligt dokumenterade avtal mellan Intric AB och AI-modelleverantörerna gäller följande lagringstider:

- **OpenAI:** API Service data lagras i max 30 dagar, därefter raderas automatiskt. Data används inte för att träna AI-modeller.
- **Anthropic:** Data lagras under avtalstiden, därefter raderas inom 30 dagar. Data "säljs" eller "delas" inte enligt US Privacy Laws.
- **Mistral, Meta (Llama):** Behandling via Airon i Sverige enligt Intricsvillkor.

Lagringstiderna gäller för driftändamål (t.ex. upptäcka missbruk, säkerställa funktionalitet). Efter att lagringstiden löpt ut raderas uppgifterna automatiskt.

C) Returnering av svar

AI-modellen returnerar sitt genererade svar till Intricsapplikationsserver, som i sin tur presenterar svaret för användaren i webbgränssnittet.

Steg 9: Lagring i Intric-plattformen

Beroende på Intricskonfiguration kan konversationshistorik lagras i Intricsdatabas hos Glesys för att:

- Möjliggöra för användaren att se tidigare konversationer
- Underlätta felsökning och support
- Säkerställa spårbarhet

Konversationshistoriken lagras kopplad till användar-ID och tidsstämpel.

Steg 10: Loggning av aktivitet

All användning av plattformen loggas för säkerhetsövervakning:

- Tidpunkt för interaktion
- Användar-ID
- Val av språkmodell
- Eventuell information om typen av aktivitet

Loggarna används för att:

- Upptäcka avvikelser eller missbruk
- Utreda eventuella incidenter
- Följa upp systemets användning

Fas 3: Kontinuerlig användning och uppdateringar

Steg 11: Uppdatering av användaruppgifter

Om användarens uppgifter förändras (t.ex. byte av e-postadress) uppdateras dessa i Intricsdatabas. Detta sker antingen:

- Automatiskt genom integration med kommunens identitetshanteringssystem
- Manuellt av systemadministratör

Steg 12: Regelbunden översyn av användarbehörighet

I enlighet med systemförvaltningsplanen genomför kommunen regelbundna översyner (minst årligen) för att säkerställa att endast behöriga medarbetare har åtkomst till plattformen. Användarkonton för medarbetare som har slutat tas bort. De som byter roll eller anställning inom kommunen tilldelas automatiskt rätt behörighetsgrupp.

Fas 4: Avslutande av användning och radering

Steg 13: Avslutande av användarkonto

När en medarbetare slutar sin anställning eller av annan anledning inte längre ska ha tillgång till Intric-plattformen avslutas användarens konto:

1. Då kontot styrs av AD, upphör kontot när användaren försvinner från HR-systemet.
2. Användarens åtkomst till plattformen stängs av
3. Konversationshistorik och annan användardata bevaras initialt för eventuell uppföljning

Steg 14: Radering av personuppgifter

Personuppgifter raderas enligt fastställda lagringstider:

Användaruppgifter (namn, e-post, användar-ID):

- Raderas senast 6 månader efter att användarkontot avslutats, om inte lagstadgade krav kräver längre lagring

Loggdata:

- Bevaras i 12 månader för säkerhetsändamål enligt kommunens informationssäkerhetspolicy
- Raderas eller anonymiseras därefter

Konversationshistorik:

- Raderas senast 3 månader efter att användarkontot avslutats
- Kan raderas tidigare på användarens begäran
- Kan anonymiseras om data ska bevaras för statistik eller utvärdering

Radering sker genom att personuppgifterna tas bort från Intricsdatabas hos Glesys. Säkerhetskopior som innehåller personuppgifterna raderas eller överskrivs inom 30 dagar i enlighet med Glesys rutiner för backup-hantering.

Steg 15: Hantering av data hos AI-modelleverantörer

Eftersom endast kontext (prompter) skickas till AI-modelleverantörer och inte användaridentifierande information, finns ingen direkt koppling mellan en specifik användares konto och data som behandlats hos dessa leverantörer.

Eventuella personuppgifter om externa personer som förekommit i prompter behandlas av AI-modelleverantörerna i enlighet med deras dataskyddspolicyer. Enligt Intricsvillkor används inte data för att träna modeller, men behandlingen för driftändamål kan variera mellan leverantörer.

Flödesschema (sammanfattning)

[Medarbetare identifieras]

↓

[Användare får information och utbildning om riktlinjer]

↓

[Användaruppgifter samlas in från kommunens system]

↓

[Användarkonto skapas i Intric hos Glesys - lagrar namn, e-post, användar-ID]

↓

[Användare loggar in via webbläsare med SSO/BankID - autentisering och loggning]

↓

[Användare väljer någon av de assistenter den har tillgång till]

↓

[Rekommendation visas: Använd svenska/EU-modeller enligt privacy by design]

↓

[Varning visas i UX om förbud mot känsliga uppgifter/sekretess]

↓

[Användare skriver prompt och bifogar eventuella filer]

↓

[Prompt skickas krypterat till vald AI-modelleverantör]

↓

[AI-modell bearbetar prompt (endast kontext och Intric server-IP delas)]

↓

[Svar returneras till Intric och visas för användare]

↓

[Konversation lagras i Intric hos Glesys]

↓

[Aktivitet loggas (tidsstämpel, användar-ID, vald modell)]

↓

[Vid användarens slut: Konto avskiljs]

↓

[Personuppgifter raderas enligt fastställda lagringstider]

Sammanfattning:

Personuppgiftsbehandlingen i Intric-plattformen följer en strukturerad process från onboarding till radering. Grundläggande användaruppgifter lagras i en dedikerad databas hos Glesys i [redacted] Vid användning av AI-modeller delas endast promptens innehåll och Intric server-IP med

modelleverantörer, aldrig användaridentifierande information. Användare rekommenderas att välja svenska/EU-baserade modeller enligt privacy by design-principen. Tydliga varningar i användargränssnittet och kommunens riktlinjer syftar till att förhindra att känsliga personuppgifter eller sekretessbelagd information hanteras. Loggning och spårbarhet säkerställer möjlighet till uppföljning och incidenthantering. Personuppgifter raderas enligt fastställda rutiner när de inte längre behövs.

3.7 Roller och ansvarsfördelning

Personuppgiftsansvarig:

Kommunstyrelsen är ensamt personuppgiftsansvarig för den behandling av anställdas personuppgifter som sker inom ramen för användningen av Intric-plattformen. För de fall personuppgiftsbehandlingen ej berör anställda är det respektive nämnd som är personuppgiftsansvarig.

Som personuppgiftsansvarig har kommunstyrelsen och berörd nämnd det fulla ansvaret för att:

- Säkerställa att behandlingen sker i enlighet med dataskyddsförordningen (GDPR)
- Fastställa ändamålen och medlen för behandlingen
- Utvärdera och hantera risker för de registrerades rättigheter och friheter
- Tillse att lämpliga tekniska och organisatoriska åtgärder vidtas
- Tillgodose de registrerades rättigheter enligt GDPR
- Rapportera personuppgiftsincidenter till Integritetsskyddsmyndigheten vid behov
- Genomföra konsekvensbedömningar och förhandssamråd vid behov

Personuppgiftsbiträden

Huvudbiträde:

Intric AB är personuppgiftsbiträde åt Lidköpings kommun och behandlar personuppgifter enligt kommunens instruktioner i enlighet med personuppgiftsbiträdesavtalet.

Intric ABs roll som personuppgiftsbiträde omfattar:

- Tillhandahålla och drifta Intric-plattformen
- Administrera användarkonton och behörigheter enligt kommunens instruktioner
- Säkerställa teknisk säkerhet och kryptering av kommunikation
- Lagra användardata och konversationshistorik i dedikerad databas
- Tillhandahålla loggning och spårbarhet
- Hantera säkerhetskopior
- Tillhandahålla teknisk support
- Radera personuppgifter enligt kommunens instruktioner när behandlingen avslutas

Underbiträden:

Intric AB anlitar följande underbiträden (underbiträdesavtal finns):

1. Glesys AB

Aspekt	Beskrivning
Roll	Datacenter och infrastrukturleverantör
Tjänster	Tillhandahåller servrar, databaser och nätverksinfrastruktur för Intric-plattformen
Geografisk placering	Sverige
Personuppgifter som behandlas	Användaruppgifter (namn, e-post, användar-ID), konversationshistorik, loggdata
Ändamål	Drift och lagring av Intric-plattformen

2. Airon (för Managed by Intric och Llama 3.3 SWE)

Aspekt	Beskrivning
Roll	Infrastrukturleverantör för hosting av Open Source-modeller
Tjänster	Tillhandahåller GPU-servrar och infrastruktur för att drifta Open Source-språkmodeller i Sverige
Geografisk placering	Sverige
Personuppgifter som behandlas	Endast kontext (prompter och bifogade filer) från användare som väljer modellerna "Managed by Intric" eller "Llama 3.3 SWE"
Ändamål	Möjliggöra AI-behandling med svensk hosting

AI-modelleverantörer:

Dessa leverantörer behandlar data endast när användare aktivt väljer att använda deras modeller. De kan betraktas som underbiträden, men har en särskild ställning eftersom de endast tar emot kontext (ej användaridentifierande information).

3. Mistral AI

Aspekt	Beskrivning
Roll	AI-modelleverantör

Aspekt	Beskrivning
Tjänster	Tillhandahåller språkmodeller för textgenerering och analys
Geografisk placering	EU/EES (Frankrike)
Personuppgifter som behandlas	• Kontext (prompter och bifogade filer) som användare skickar • IP-adress från Intricsserver **INTE:** Namn, e-post eller användar-ID
Skyddsåtgärder	• Behandling inom EU/EES • Krypterad kommunikation • Endast kontext delas, inte användaridentifierande information
Ändamål	AI-behandling av prompter för att generera svar
Kommentar	**Rekommenderad modell** enligt privacy by design-principen

4. OpenAI (OpenAI GPT-modeller)

Aspekt	Beskrivning
Roll	AI-modelleverantör
Tjänster	Tillhandahåller språkmodeller för textgenerering och analys
Geografisk placering	USA (OpenAI OpCo, LLC, 1960 Bryant Street, San Francisco, CA 94110)
Personuppgifter som behandlas	• Kontext (prompter och bifogade filer) som användare skickar • IP-adress från Intricsserver (inte användarens IP) **INTE:** Namn, e-post eller användar-ID
Skyddsåtgärder för tredjelandsöverföring	• **Standardavtalsklausuler (SCC)** Module Two (Controller to Processor) via Data Processing Addendum mellan Intric AB och OpenAI (daterat 24 januari 2024) • OpenAI är INTE certifierad enligt EU-U.S. Data Privacy Framework • **Data retention:** Max 30 dagar för API Service data, därefter raderas • **Ej träning:** Data används inte för att träna AI-modeller • **Säkerhetscertifieringar:** SOC 2 Type II • Endast kontext (ej användaridentifierande info) delas • Användare kan välja EU/EES-alternativ • Förbud mot känsliga personuppgifter minskar risken • **HÄNVISNING:** Se avsnitt 4.4 för fullständig bedömning

Aspekt	Beskrivning
Ändamål	AI-behandling av prompter för att generera svar. Har mycket hög intelligens och klarar fler komplexa uppgifter än Open Source-modellerna.
Kommentar	Användare väljer aktivt denna modell och är informerade om tredjelandsöverföring

5. Anthropic (Claude-modeller)

Aspekt	Beskrivning
Roll	AI-modelleverantör
Tjänster	Tillhandahåller språkmodeller för textgenerering och analys
Geografisk placering	USA
Personuppgifter som behandlas	• Kontext (prompter och bifogade filer) som användare skickar • IP-adress från Intricsserver **INTE:** Namn, e-post eller användar-ID
Skyddsåtgärder för tredjelandsöverföring	• **Standardavtalsklausuler (SCC)** Module Two (Controller to Processor) och Module Three (Processor to Sub-Processor) via Data Processing Addendum (ikraftträdande 24 februari 2025) • Anthropic är INTE certifierad enligt EU-U.S. Data Privacy Framework • **Data retention:** 30 dagar efter avslutad behandling, därefter raderas • **Ej "försäljning":** Data "säljs" eller "delas" inte enligt US Privacy Laws • **Säkerhetscertifieringar:** SOC 2, AES-256 kryptering, TLS 1.2+ • Endast kontext (ej användaridentifierande info) delas • Användare kan välja EU/EES-alternativ • Förbud mot känsliga personuppgifter minskar risken • **HÄNVISNING:** Se avsnitt 4.4 för fullständig bedömning
Ändamål	AI-behandling av prompter för att generera svar. Har mycket hög intelligens och klarar fler komplexa uppgifter än Open Source-modellerna.
Kommentar	Användare väljer aktivt denna modell och är informerade om tredjelandsöverföring

6. Meta (Llama 3.3 SWE)

Aspekt	Beskrivning
Roll	AI-modelleverantör (Open Source)
Tjänster	Tillhandahåller Open Source-modell specialiserad för svenska språket
Geografisk placering	Sverige (hostning via Airon)
Personuppgifter som behandlas	• Kontext (prompter och bifogade filer) som användare skickar **INTE:** Namn, e-post eller användar-ID
Skyddsåtgärder	• Behandling i Sverige • Krypterad kommunikation • Endast kontext delas, inte användaridentifierande information
Ändamål	AI-behandling av prompter för att generera svar på svenska
Kommentar	**Rekommenderad modell** enligt privacy by design-principen

Avtalsdokumentation

Följande avtalsdokument reglerar ansvarsfördelningen:

1. Personuppgiftsbiträdesavtal mellan Lidköpings kommun och Intric AB

Detta avtal reglerar:

- Intric ABs skyldigheter som personuppgiftsbiträde enligt artikel 28 GDPR
- Vilka personuppgifter som behandlas och för vilka ändamål
- Säkerhetsåtgärder som Intric AB ska vidta
- Rutiner för hantering av personuppgiftsincidenter
- Intric ABs skyldighet att biträda kommunen vid hantering av registrerades rättigheter
- Villkor för anlitande av underbiträden
- Rutiner för radering av personuppgifter när uppdraget avslutas
- Revisionsrättigheter för kommunen

2. Underbiträdesavtal mellan Intric AB och Glesys AB

Reglerar Glesys ABs roll som underbiträde för infrastruktur och lagring.

3. Underbiträdesavtal mellan Intric AB och Airon

Reglerar Airons roll som underbiträde för hosting av Open Source-modeller i Sverige.

4. Avtal/villkor med AI-modelleverantörer

Intric AB har tecknat formella Data Processing Agreements med AI-modelleverantörer som reglerar behandlingen av data:

Dokumenterade avtal:

- **OpenAI:** Data Processing Addendum daterat 24 januari 2024 (undertecknat av Intric AB 8 maj 2025) med EU SCCs Module Two
- **Anthropic:** Data Processing Addendum ikraftträdande 24 februari 2025 med EU SCCs Module Two och Module Three
- **Mistral, Meta (Llama):** Behandling via Airons infrastruktur i Sverige enligt Intricsvillkor

Kommunens insyn:

Lidköpings kommun har genom Intric AB tillgång till de fullständiga DPA:erna med OpenAI och Anthropic, vilka specificerar:

- Exakta lagringstider (30 dagar)
- Säkerhetsåtgärder och certifieringar (SOC 2, ISO 27001)
- Förbud mot träning på customer data
- Subprocessor-listor och ändringsrutiner
- Incidenthantering och anmälningsplikt

För amerikanska leverantörer (OpenAI, Anthropic) skyddas överföringen av **standardavtalsklausuler (SCC)** enligt EU-kommissionens beslut från 4 juni 2021, då dessa leverantörer **inte är certifierade enligt EU-U.S. Data Privacy Framework**. Se **avsnitt 4.4** för fullständig bedömning av skyddsåtgärder och risker.

Mottagare av personuppgifter

Utöver de personuppgiftsbiträden som anges ovan kommer personuppgifter inte att delas med andra externa mottagare, förutom i de fall då:

- Lagstadgade skyldigheter kräver det (t.ex. polisanmälan vid misstanke om brott)
- Registrerade begär ut sina uppgifter enligt GDPR artikel 15
- Integritetsskyddsmyndigheten och DSO begär information inom ramen för tillsyn

Sammanfattning av roller

Aktör	Roll	Ansvar
Kommunstyrelsen	Personuppgiftsansvarig	Fullständigt ansvar för att behandlingen följer GDPR, fastställer ändamål och medel, hanterar risker

Aktör	Roll	Ansvar
Intric AB	Personuppgiftsbiträde	Tillhandahåller plattform, administrerar konton, säkerställer teknisk säkerhet enligt instruktioner från kommunen
Glesys AB	Underbiträde (till Intric)	Datacenter, servrar och lagring av data i Sverige
Airon	Underbiträde (till Intric)	Hosting av Open Source-modeller i Sverige
Mistral AI	Underbiträde/AI-leverantör	Behandlar endast kontext (prompter) för AI-generering inom EU, ingen användaridentifierande information. **Rekommenderad.**
Meta (Llama 3.3 SWE)	Underbiträde/AI-leverantör	Open Source-modell hostad i Sverige via Airon, behandlar endast kontext. **Rekommenderad.**
OpenAI	Underbiträde/AI-leverantör	Behandlar endast kontext (prompter) för AI-generering i USA, ingen användaridentifierande information. Se avsnitt 4.4 för skyddsåtgärder.
Anthropic	Underbiträde/AI-leverantör	Behandlar endast kontext (prompter) för AI-generering i USA, ingen användaridentifierande information. Se avsnitt 4.4 för skyddsåtgärder.

Denna tydliga ansvarsfördelning med dokumenterade avtal säkerställer att rollerna är definierade och att varje part känner till sina skyldigheter enligt dataskyddsförordningen.

Steg 4. Rättslig analys

4.1 Gällande regelverk

Följande regelverk är tillämpliga för den aktuella personuppgiftsbehandlingen:

Dataskydd och integritet

Europaparlamentets och rådets förordning (EU) 2016/679 (GDPR)

- Grundläggande regelverk för behandling av personuppgifter
- Reglerar personuppgiftsansvar, laglighet, dataskyddsprinciper, registrerades rättigheter, säkerhetsåtgärder, konsekvensbedömning och tredjelandsöverföringar

Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (Dataskyddslagen)

- Kompletterar GDPR med svensk reglering

- Reglerar t.ex. behandling av personnummer (3 kap. 10 §)

Offentlighets- och sekretesslagen (2009:400)

- Reglerar sekretess för uppgifter som hanteras inom kommunal verksamhet
- Avgörande för att avgränsa vilka uppgifter som INTE får behandlas i Intric-plattformen

Informationssäkerhet

? Ta bort

Cybersäkerhetslagen

?

Arbetsrätt och medarbetaruppgifter

Arbetsmiljölagen (1977:1160)

- Relevant för att säkerställa att medarbetare har en säker arbetsmiljö även vid användning av nya digitala verktyg

Avtal och upphandling

Lagen (2016:1145) om offentlig upphandling (LOU)

- Om Intric-plattformen har upphandlats enligt LOU

Kommunalrättsliga bestämmelser

Kommunallagen (2017:725)

- Reglerar kommunens verksamhet och ansvar

Relevanta standards och certifieringar

ISO/IEC 27001:2022 – Standard för ledningssystem för informationssäkerhet

- Intric AB har certifiering enligt denna standard (certifikat ACCISMS2025110188)
- Kommunen har ett ledningssystem för informationssäkerhet

ISO/IEC 27018 – Code of practice for protection of personally identifiable information (PII) in public clouds

- Relevant för molnbaserade tjänster

ISO/IEC 27701 – Extension to ISO/IEC 27001 for privacy information management

- Kompletterande standard för integritetsskydd

Branschpraxis och vägledning

Integritetsskyddsmyndighetens (IMY) vägledning

- Riktlinjer om konsekvensbedömning
- Vägledning om behandling av personuppgifter vid användning av molntjänster
- Vägledning om AI och personuppgiftsbehandling

Europeiska dataskyddsstyrelsens (EDPB) riktlinjer

- Riktlinjer om behandling av personuppgifter vid användning av molntjänster
- Riktlinjer om AI och automatiserat beslutsfattande

Kommunala styrdokument

Lidköpings kommuns informationssäkerhetspolicy (2024)

- Fastställer krav på säkerhetsnivåer och skyddsåtgärder

Riktlinjer för artificiell intelligens (AI) – Lidköpings kommunkoncern

- Fastställer grundläggande principer för AI-användning
- Specificerar vilka uppgifter som får och inte får behandlas
- Tydliggör medarbetares och chefers ansvar
- Reglerar etiskt användande, transparens och hållbarhet

Informationssäkerhet för medarbetare och förtroendevalda – riktlinje (2024)

- Kompletterar informationssäkerhetspolicyn

Förvaltningsplan Intric AI 2025-2026

- Beskriver roller, ansvar och aktiviteter för förvaltning av Intric-plattformen
- Reglerar support, utbildning, förändringshantering och livscykelhantering

Dataskyddsförordningen

Sammanfattning:

Behandlingen regleras främst av GDPR och svensk dataskyddslagstiftning. Offentlighets- och sekretesslagen är avgörande för att avgränsa vilka uppgifter som inte får behandlas i plattformen. Internationella överföringar till USA för vissa AI-modeller regleras av standardavtalsklausuler (SCC). Intric AB och Glesys AB har relevanta ISO-certifieringar som stärker förtroendet för deras säkerhetsarbete. Kommunens egna styrdokument kompletterar den externa regleringen och skapar interna krav för ansvarsfull användning.

AI-förordningen (EU) 2024/1689

Europaparlamentets och rådets förordning (EU) 2024/1689 om harmoniserade regler för artificiell intelligens (AI-förordningen) är direkt tillämplig och införs stegvis under 2025–2027. Kommunen betraktas som ”användare” enligt AI-förordningens terminologi.

Den beskrivna användningen bedöms INTE klassificeras som ”hög risk” enligt bilaga 3, eftersom AI används som stödverktyg, automatiserat beslutsfattande är förbjudet, och individnära ärenden inte hanteras.

Kommunen säkerställer att systemet inte används i hög-risk-sammanhang, att mänsklig kontroll upprätthålls, att användare har tillräcklig kompetens, och att transparenskrav uppfylls. Riskklassificeringen dokumenteras och följs upp löpande (se avsnitt 10.1).

AI-förordningen är ett separat men kompletterande regelverk till GDPR och integreras i kommunens övergripande AI- och informationssäkerhetsstyrning.

4.2 Dataskyddsprinciperna och den rättsliga grunden för behandlingen

Principen om laglighet, korrekthet och öppenhet

Laglighet

Behandlingen av personuppgifter i Intric-plattformen ska ske i enlighet med dataskyddsförordningen och kompletterande lagstiftning. För att behandlingen ska vara laglig krävs att den har stöd i en rättslig grund enligt artikel 6 GDPR.

Rättslig grund för behandlingen:

Behandlingen av personuppgifter i Intric-plattformen vilar på följande rättsliga grunder:

1. För behandling av medarbetares personuppgifter (namn, e-post, användar-ID, loggdata):

Artikel 6.1 e GDPR – Uppgift av allmänt intresse

Kommunen har ett behov av att tillhandahålla sina medarbetare moderna och effektiva arbetsverktyg för att kunna fullgöra sitt uppdrag gentemot invånarna på ett kostnadseffektivt och kvalitativt sätt. Nödvändighets- och proportionalitetsbedömning:

Kommunens intresse av behandlingen:

- Effektivisera textproduktion och administration
- Höja kvaliteten i kommunikation med invånare
- Ge medarbetare tillgång till modern teknik
- Öka produktiviteten och minska kostnader för externa konsulter

Medarbetarnas intressen och rättigheter:

- Skydd för personuppgifter (grundläggande identitetsuppgifter)
- Integritet i arbetslivet
- Skydd mot otillbörlig övervakning

Bedömning:

Behandlingen av medarbetares grundläggande identitetsuppgifter för att ge dem åtkomst till ett arbetsverktyg bedöms vara proportionerlig och medföra låg risk för medarbetarnas fri- och rättigheter. Medarbetarna befinner sig i beroendeställning, men användningen av Intric är frivillig och utgör ett komplement till befintliga arbetssätt.

De personuppgifter som behandlas är begränsade till namn, e-postadress och användar-ID – uppgifter som redan behandlas i många andra system inom kommunen (t.ex. e-postsystem, intranät). Loggning sker för säkerhetsändamål och är nödvändig för att upptäcka missbruk och skydda både medarbetare och kommun.

Kommunen har vidtagit tekniska och organisatoriska åtgärder för att minimera riskerna, inklusive kryptering, begränsad datalagring och tydliga riktlinjer för användning.

Slutsats: Behandlingen av medarbetares grundläggande identitetsuppgifter är nödvändig för att utföra en uppgift av allmänt intresse och är proportionerlig i förhållande till ändamålet. Den rättsliga grunden är artikel 6.1 e GDPR med stöd i kommunallagen (2017:725).

2. För personuppgifter om externa personer som kan förekomma i användares prompter:

Eftersom användare själva aktivt väljer att inkludera personuppgifter om externa personer (namn, e-post, telefonnummer) i sina prompter, och denna användning sker inom ramen för kommunens arbetsuppgifter gentemot externa parter, bedöms följande rättsliga grunder vara tillämpliga beroende på sammanhanget:

Artikel 6.1 e GDPR – Uppgift av allmänt intresse

Behandlingen av externa personers kontaktuppgifter sker inom ramen för kommunens ordinarie verksamhet (projekt, kommunikation, samverkan) och grundas på artikel 6.1 e.

Kommunens behov av behandlingen:

- Effektivisera kommunikation och textproduktion
- Förbättra kvaliteten i dokumentation och rapporter
- Underlätta samverkan med externa parter

Proportionalitetsbedömning:

- Skydd för personuppgifter (namn, kontaktuppgifter)
- Rätt till information om behandlingen
- Skydd mot oväntad eller otillbörlig behandling

Bedömning:

De personuppgifter om externa personer som kan förekomma i Intric är begränsade till grundläggande kontaktuppgifter (namn, e-post, telefon). Dessa uppgifter används endast för att skapa texter och dokument som är relaterade till kommunens ordinarie verksamhet. Behandlingen medför låg risk eftersom:

- Känsliga personuppgifter och sekretess är förbjudna enligt riktlinjerna

- Uppgifterna används endast för specificerade ändamål (t.ex. projektdokumentation, kommunikation)
- Externa personer kan rimligen förvänta sig att deras kontaktuppgifter hanteras av kommunen i samband med samarbeten och kommunikation

Slutsats: För externa personers uppgifter är den rättsliga grunden artikel 6.1 e (uppgift av allmänt intresse) när behandlingen sker inom ramen för kommunens ordinarie verksamhet.

Korrekthet

Behandlingen ska ske på ett rättvist, skäligt och rimligt sätt gentemot de registrerade.

Åtgärder för att säkerställa korrekthet:

- **Frivillighet för medarbetare:** Användning av Intric är frivillig och medarbetare kan välja att utföra samma arbetsuppgifter med andra metoder.
- **Tydliga riktlinjer:** Kommunen har fastställt riktlinjer som tydligt anger vad som är tillåtet och inte tillåtet att behandla i plattformen.
- **Privacy by design:** Kommunen rekommenderar användning av svenska/EU-baserade modeller som förstahandsval för personuppgifter.
- **Proportionalitet:** Endast grundläggande identitetsuppgifter behandlas för användaradministration, inte känsliga eller detaljerade uppgifter.
- **Transparens:** Medarbetare och externa personer informeras om behandlingen (se nedan under "Öppenhet").
- **Icke-diskriminerande:** Behandlingen sker på samma sätt för alla medarbetare som får tillgång till plattformen, utan diskriminering.

Öppenhet

De registrerade ska få tydlig och lättillgänglig information om hur deras personuppgifter behandlas.

Åtgärder för att säkerställa öppenhet:

För medarbetare:

Medarbetare som får tillgång till Intric informeras om behandlingen genom:

- **Information på AI-portal:** Vid onboarding får användare information om hur deras personuppgifter behandlas, vilka rättsliga grunder som används, hur länge uppgifterna lagras och vilka rättigheter de har.
- **Utbildningstillfällen:** Basutbildning i AI, instruktionsfilmer och utbildningsmaterial där dataskyddsaspekter ingår.
- **Intranät:** Information om Intric och personuppgiftsbehandling publiceras på kommunens intranät.

- **Kontaktuppgifter:** Tydliga kontaktuppgifter till dataskyddsombud och Systemförvaltare för frågor om behandlingen.

Informationen inkluderar:

- Vem som är personuppgiftsansvarig (Kommunstyrelsen och/eller berörd nämnd)
- Vilka personuppgifter som behandlas (namn, e-post, användar-ID, loggdata)
- Ändamål med behandlingen
- Rättslig grund (uppgift av allmänt intresse enligt artikel 6.1 e GDPR, med stöd i kommunallagen)
- Mottagare av personuppgifter (Intric AB, underleverantörer, AI-modelleverantörer vid aktiv användning)
- Information om vilka modeller som behandlar data i Sverige/EU respektive USA
- Lagringstid
- Registrerades rättigheter (tillgång, rättelse, radering, begränsning, invändning, klagomål till IMY)

För externa personer:

Eftersom externa personer vars uppgifter kan förekomma i användarinteraktioner inte har direkt kontakt med Intric-plattformen, informeras de genom:

- **Kommunens allmänna integritetspolicy:** Publicerad på kommunens webbplats och anger hur personuppgifter kan komma att behandlas inom kommunens verksamhet, inklusive användning av externa verktyg.
- **Specifik information vid relevant tillfälle:** Om en extern person är involverad i ett projekt eller samarbete där Intric används, kan information lämnas vid behov.

Informationen anger:

- Att kommunen använder digitala verktyg, inklusive AI-baserade tjänster, för att effektivisera sitt arbete
- Att grundläggande kontaktuppgifter kan behandlas i dessa verktyg
- Kontaktuppgifter för frågor (dataskyddsombud)

Sammanfattning – Laglighet, korrekthet och öppenhet:

Behandlingen har tydlig och giltig rättslig grund i artikel 6.1 e GDPR (uppgift av allmänt intresse) med stöd i kommunallagen (2017:725). Denna rättsliga grund tillämpas konsekvent för såväl medarbetares användaruppgifter som för externa personers kontaktuppgifter som kan förekomma i användarinteraktioner. Behandlingen är rättvis och proportionerlig då endast nödvändiga uppgifter behandlas för specificerade ändamål. Öppenhet säkerställs genom tydlig information till både medarbetare och externa personer via flera kanaler.

Rättslig grund för behandlingen (detaljerad tabell)

Nr	Beskrivning av behandlingen	Personuppgifter som behandlas	Rättslig grund	Kommentar
01	Skapande och administration av användarkonton i Intric-plattformen	Namn, e-postadress, användar-ID	Artikel 6.1 e – Uppgift av allmänt intresse	Behandlingen är nödvändig för att ge medarbetare åtkomst till ett arbetsverktyg som effektiviserar fullgörandet av kommunens offentliga uppdrag. Rättslig grund med stöd i kommunallagen (2017:725). Proportionerligt då behandlingen begränsas till grundläggande identitetsuppgifter och användningen är frivillig.
02	Loggning av användaraktivitet (inloggningar, val av modell, tidsstämplar)	Användar-ID, tidsstämplar, aktivitetsdata	Artikel 6.1 e – Uppgift av allmänt intresse	Nödvändigt för säkerhetsövervakning, att upptäcka missbruk och utreda incidenter. Loggning är en grundläggande säkerhetsåtgärd enligt artikel 32 GDPR och kommunens informationssäkerhetspolicy. Proportionerligt då loggningen begränsas till säkerhetsändamål.
03	Lagring av konversationshistorik i Intricsplattformen	Användar-ID, prompter, genererade svar, tidsstämplar	Artikel 6.1 e – Uppgift av allmänt intresse	Nödvändigt för att möjliggöra för användare att se tidigare konversationer och underlätta felsökning inom ramen för kommunens verksamhet. Proportionerligt med hänsyn till begränsad lagringstid (3 månader efter avslutande). Användare kan begära radering.
04	Användning av AI-modeller för textproduktion inom kommunens uppdrag	Personuppgifter om externa personer (namn, e-post, telefon) som användare inkluderar i prompter	Artikel 6.1 e – Uppgift av allmänt intresse	Behandlingen av externa personers kontaktuppgifter sker inom ramen för kommunens ordinarie verksamhet (projekt, kommunikation, samverkan) och grundas på artikel 6.1 e.
05	Användning av AI-modeller för administrativa uppgifter	Personuppgifter om externa personer (namn, e-post, telefon) som användare inkluderar i prompter	Artikel 6.1 e – Uppgift av allmänt intresse	När behandlingen inte direkt utgör myndighetsutövning men är nödvändig för kommunens administrativa effektivitet. Låg risk och proportionerlig behandling.
06	Säkerhetskopiering av databas hos Glesys AB	Namn, e-post, användar-ID, konversationshistorik, loggdata	Artikel 6.1 e – Uppgift av allmänt intresse	Nödvändigt för att säkerställa tillgänglighet och återställning vid incident. Säkerhetskopiering är en grundläggande säkerhetsåtgärd.
07	Överföring av kontext (prompter) till AI-modelleverantörer i Sverige/EU (Managed by Intric, Llama, Mistral)	Kontext (prompter och bifogade filer)	Artikel 6.1 e – Uppgift av allmänt intresse	Endast kontext delas, inte användaridentifierande information. Behandling inom Sverige/EU. Rekommenderade modeller enligt privacy by design. Behandlingen understöds av SCC-moduler och att leverantörerna raderar data efter högst 30 dagar.

Nr	Beskrivning av behandlingen	Personuppgifter som behandlas	Rättslig grund	Kommentar
08	Överföring av kontext (prompter) till AI-modelleverantörer i USA (OpenAI, Anthropic)	Kontext (prompter och bifogade filer)	Artikel 6.1 e – Uppgift av allmänt intresse	Endast kontext delas, inte användaridentifierande information. Användare väljer aktivt dessa modeller. Behandlingen understöds av SCC-moduler och att leverantörerna raderar data efter högst 30 dagar.

Rättsligt stöd för behandling av vissa kategorier av personuppgifter

Denna behandling omfattar **INTE** särskilda kategorier av personuppgifter enligt artikel 9 GDPR (känsliga personuppgifter) eller uppgifter om lagöverträdelser enligt artikel 10 GDPR.

Det är uttryckligen förbjudet enligt kommunens riktlinjer att behandla sådana uppgifter i Intric-plattformen. Tekniska varningar i användargränssnittet påminner användare om detta förbud.

Personnummer:

Personnummer behandlas INTE i Intric-plattformen för användaradministration. Om personnummer skulle förekomma i en användares prompt av misstag (vilket strider mot riktlinjerna), regleras behandlingen av 3 kap. 10 § dataskyddslagen, som kräver att behandlingen är "klart motiverad" med hänsyn till ändamålet, vikten av en säker identifiering eller något annat beaktansvärt skäl.

Eftersom syftet med Intric inte är att hantera personnummer, ska användare instrueras att aldrig inkludera sådana uppgifter.

Principen om ändamålsbegränsning

Personuppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål.

Åtgärder för att säkerställa ändamålsbegränsning:

1. Tydligt definierade ändamål:

Ändamålen med behandlingen är noggrant specificerade i avsnitt 3.4 och omfattar endast:

- Användaradministration för att ge medarbetare åtkomst till plattformen
- Användning av AI-modeller för specificerade arbetsuppgifter inom avgränsade verksamhetsområden (kommunikation, administration, kompetensutveckling, analys, etc.)
- Säkerhetsövervakning och loggning för att upptäcka missbruk och incidenter

2. Dokumenterade begränsningar:

Kommunens riktlinjer för användning av Intric anger tydligt:

- Vilka typer av arbetsuppgifter som får stödjas med AI-verktyget
- Vilka typer av information som inte får behandlas (känsliga personuppgifter, sekretess)

- Att plattformen endast får användas för arbetsrelaterade ändamål, inte för privata syften

3. Tekniska åtgärder:

- **Varningar i användargränssnittet:** Påminner användare om begränsningarna innan de skickar en prompt.
- **Loggning:** Ger möjlighet att upptäcka om plattformen används för oförenliga ändamål.

4. Utbildning och information:

Medarbetare utbildas om ändamålen med Intric och får tydlig information om vad som är tillåtet och inte tillåtet genom:

- Basutbildning i AI
- Instruktionsfilmer
- Riktlinjerna för AI i kommunkoncernen

5. Uppföljning:

Systemförvaltaren och dataskyddsombud följer regelbundet upp användningen för att säkerställa att plattformen används i enlighet med fastställda ändamål.

6. Förbud mot vidareutnyttjande:

Personuppgifter som behandlas i Intric får inte användas för andra ändamål än de specificerade. Exempelvis:

- Loggdata får inte användas för prestandaövervakning av enskilda medarbetare
- Konversationshistorik får inte användas för att träna egna AI-modeller utan uttryckligt samtycke och ny rättslig grund

Sammanfattning – Ändamålsbegränsning:

Ändamålen är tydligt definierade, dokumenterade och begränsade till specificerade arbetsuppgifter. Tekniska och organisatoriska åtgärder säkerställer att behandlingen inte sker för oförenliga ändamål.

Principen om uppgiftsminimering

Personuppgifter ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas.

Åtgärder för att säkerställa uppgiftsminimering:

1. Begränsade användaruppgifter:

För användaradministration behandlas endast de personuppgifter som är absolut nödvändiga enligt principen om minsta behörighet (Least Privilege) som definieras i Intrics Access Control Policy:

- För- och efternamn (för identifiering)
- E-postadress (för kommunikation och inloggning)
- Användar-ID (teknisk identifierare)

Inga ytterligare uppgifter som personnummer, födelsedata, adress, telefonnummer eller arbetsroll lagras i Intric-plattformen.

2. Minimering av data till AI-modelleverantörer:

När användare interagerar med AI-modeller delas endast:

- Kontext (prompter och bifogade filer) som användaren aktivt väljer att dela

INTE:

- Användarens namn
- Användarens e-postadress
- Användar-ID
- Användarens IP-adress

Detta minimerar exponeringen av personuppgifter gentemot externa AI-leverantörer.

3. Begränsning av personuppgifter i användarinteraktioner:

Kommunens Riktlinjer för artificiell intelligens (AI) anger att användare endast får inkludera grundläggande kontaktuppgifter (namn, e-post, telefon) om det är nödvändigt för ändamålet. Känsliga personuppgifter och sekretessbelagd information är förbjudna.

Användare uppmanas att:

- Överväga om personuppgifter verkligen behövs i prompten
- Anonymisera eller pseudonymisera uppgifter när det är möjligt (Intric har Data Masking Service för detta ändamål)
- Använda fiktiva exempel istället för verkliga personer när det är lämpligt

4. Privacy by design:

Kommunen rekommenderar användning av svenska/EU-baserade modeller (Managed by Intric, Llama 3.3 SWE, Mistral) som förstahandsval för arbetsuppgifter som kan innehålla personuppgifter. Detta minimerar tredjelandsöverföringar och ökar kontrollen över data.

5. Alternativa arbetssätt har övervägts:

Kommunen har övervägt om det finns alternativa metoder för att uppnå samma effektivitetsvinster utan att behandla personuppgifter. Bedömningen är att:

- Manuell textproduktion utan AI-stöd skulle vara möjlig, men betydligt mer tidskrävande och kostsam
- Användning av AI-verktyg utan att lagra några användaruppgifter alls (helt anonymt) skulle inte vara tekniskt möjligt ur ett säkerhetsperspektiv, då spårbarhet och åtkomstkontroll krävs
- Den valda lösningen med minimala användaruppgifter och tydliga begränsningar bedöms vara den mest proportionerliga

6. Loggning begränsas till säkerhetsändamål:

Loggning sker endast i den utsträckning som är nödvändig för säkerhetsövervakning och incidenthantering. Detaljerad övervakning av medarbetares individuella användningsmönster genomförs inte.

Sammanfattning – Uppgiftsminimering:

Behandlingen begränsas till absolut nödvändiga personuppgifter. Användaruppgifter för administration är minimala (namn, e-post, användar-ID). Delning med AI-leverantörer begränsas till kontext utan användaridentifierande information. Kommunens riktlinjer och tekniska varningar minskar risken för att onödiga personuppgifter inkluderas i användarinteraktioner. Privacy by design-principen implementeras genom rekommendation av svenska/EU-baserade modeller.

Principen om riktighet

Personuppgifter ska vara riktiga och, om nödvändigt, uppdaterade. Felaktiga personuppgifter ska raderas eller rättas utan dröjsmål.

Åtgärder för att säkerställa riktighet:

1. Insamling från tillförlitlig källa:

Användaruppgifter (namn, e-post) samlas in från kommunens befintliga system (HR-system, Active Directory) vilket säkerställer att uppgifterna är korrekta vid tidpunkten för skapandet av kontot.

2. Automatisk uppdatering:

Om Intric integreras med kommunens identitetshanteringssystem (t.ex. Active Directory) synkroniseras ändringar automatiskt. Om en medarbetare byter e-postadress uppdateras detta även i Intric.

3. Manuell uppdatering vid behov:

Om automatisk synkronisering inte är implementerad, säkerställer Systemförvaltaren att användaruppgifter uppdateras manuellt vid förändringar (t.ex. namnbyte, byte av e-postadress).

4. Registrerades rätt till rättelse:

Medarbetare kan kontakta Systemförvaltaren eller dataskyddsombud för att begära rättelse av felaktiga uppgifter i Intric-plattformen.

5. Regelbunden översyn:

I samband med regelbundna översyner av användarbehörigheter (minst årligen) kontrolleras även att användaruppgifterna är korrekta och uppdaterade.

6. Riktighet i användarinteraktioner:

För personuppgifter om externa personer som användare inkluderar i prompter ansvarar användaren själv för att uppgifterna är korrekta. Kommunens riktlinjer påminner om detta ansvar.

Sammanfattning – Riktighet:

Användaruppgifter hålls korrekta genom insamling från tillförlitliga källor, automatisk eller manuell uppdatering vid ändringar och möjlighet för registrerade att begära rättelse. Regelbundna översyner säkerställer att uppgifterna förblir aktuella.

Principen om lagringsminimering

Personuppgifter får inte förvaras i en form som möjliggör identifiering under längre tid än vad som är nödvändigt för de ändamål för vilka de behandlas.

Åtgärder för att säkerställa lagringsminimering:

1. Fastställda lagringstider:

Kommunen fastställer följande lagringstider för personuppgifter i Intric-plattformen:

Kategori av personuppgifter	Lagringstid	Motivering
Användaruppgifter (namn, e-post, användar-ID)	Så länge användarkontot är aktivt + **6 månader** efter avslutande	Möjliggör uppföljning och felsökning efter att kontot avslutats. Efter 6 månader raderas uppgifterna.
Konversationshistorik	Så länge användarkontot är aktivt + **3 månader** efter avslutande, ELLER på begäran av användare	Användare kan begära radering av sin konversationshistorik när som helst. Efter 3 månader från avslutande raderas automatiskt.
Loggdata (säkerhetshändelser, inloggningar)	**12 månader**	Nödvändigt för säkerhetsövervakning och incidentutredningar enligt kommunens informationssäkerhetspolicy. Efter 12 månader anonymiseras eller raderas loggdata.
Säkerhetskopior	Samma lagringstid som originaldata + maximal kvarhållningstid för backup (**30 dagar**)	Säkerhetskopior överskrivs löpande enligt Glesys rutiner. Personuppgifter som raderats från produktionssystemet kommer även att försvinna från backupen inom 30 dagar.

2. Automatisk gallring:

Intric-plattformen konfigureras så att personuppgifter automatiskt raderas när lagringstiderna har löpt ut. Systemförvaltaren ansvarar för att säkerställa att denna funktion är aktiv och fungerar korrekt.

3. Manuell gallring vid behov:

Om en medarbetare begär radering av sin konversationshistorik innan lagringstiden har löpt ut, genomförs manuell radering av Systemförvaltaren eller via självbetjäningsfunktion i plattformen (om tillgänglig).

4. Regelbunden översyn av lagringstider:

Kommunen ser över fastställda lagringstider minst vart tredje år för att säkerställa att de fortfarande är motiverade och proportionerliga.

5. Ingen lagring för oförenliga ändamål:

Personuppgifter från Intric får inte kopieras eller exporteras för andra ändamål än de ursprungliga utan ny rättslig grund och information till de registrerade.

Sammanfattning – Lagringsminimering:

Tydliga lagringstider är fastställda och motiverade utifrån ändamålen. Automatisk och manuell gallring säkerställer att uppgifter raderas när de inte längre behövs. Regelbunden översyn garanterar att lagringstiderna förblir proportionerliga.

Principen om integritet och konfidentialitet

Personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inklusive skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.

Tekniska säkerhetsåtgärder:

1. Kryptering:

- **SSL/TLS-kryptering:** All kommunikation mellan användares enheter och Intric-plattformen, mellan Intricswebbserver och applikationsserver, samt mellan Intric och externa AI-modelleverantörer sker krypterat med SSL/TLS.
- **Kryptering av data i vila:** Personuppgifter som lagras i Intricsdatabas hos Glesys är krypterade i enlighet med Glesys säkerhetsstandarder.

2. Åtkomstkontroll och autentisering:

- **Inloggningskrav:** Användare måste autentisera sig med SSO och BankID för att få åtkomst till Intric-plattformen.
- **Multifaktorautentisering (MFA):** Implementerat via BankID.
- **Rollbaserad åtkomstkontroll:** Endast användare med aktiva användarkonton får åtkomst till plattformen. Administratörer har separata behörigheter för administration av systemet.

3. Loggning och spårbarhet:

- **Säkerhetsloggning:** All användaraktivitet loggas, inklusive inloggningar, val av modell och tidsstämplar.
- **Övervakning:** Systemförvaltaren övervakar loggar för att upptäcka avvikelser eller misstänkt aktivitet via SIEM-system.
- **Incidenthantering:** Rutiner finns för att hantera och rapportera personuppgiftsincidenter enligt artikel 33-34 GDPR.

4. Nätverkssäkerhet:

- **Brandväggar och intrångsskydd:** Glesys datacenter använder brandväggar och intrångsskyddssystem för att skydda mot externa hot.

- **Isolerad databas:** Lidköpings kommuns data lagras i en dedikerad databas, isolerad från andra tenanter på samma server.

5. Säkerhetskopiering:

- **Regelbundna backuper:** Dagliga inkrementella och veckovisa fulla säkerhetskopior av databasen görs av Glesys för att säkerställa återställning vid incident.
- **Skyddade backuper:** Säkerhetskopiorna lagras krypterat och åtkomst är begränsad.
- **Kvartalsvis testning:** Återställning testas regelbundet.

6. Uppdateringar och patchning:

- **Säkerhetsuppdateringar:** Intric AB ansvarar för att hålla plattformen uppdaterad med säkerhetspatchar och uppdateringar.

7. Begränsad datatillgång hos Intric AB:

- **Endast systemansvariga:** Endast systemansvariga på Intric AB har datatillgång i läsbar format för support- och driftändamål.
- **Konfidentialitetsavtal:** Intricsanställda är bundna av konfidentialitetsavtal och instruktioner om hantering av kunddata.

Organisatoriska säkerhetsåtgärder:

1. Personuppgiftsbiträdesavtal:

- **Tydliga villkor:** PUB-avtalet med Intric AB reglerar säkerhetsåtgärder, ansvarsfördelning och villkor för behandlingen.
- **Underbiträdesavtal:** Intric har underbiträdesavtal med Glesys, Airon och AI-modelleverantörer som reglerar deras säkerhetsansvar.

2. Riktlinjer och instruktioner:

- **Riktlinjer för artificiell intelligens (AI):** Kommunens fastställda riktlinjer anger tydligt vilka typer av information som inte får behandlas (känsliga personuppgifter, sekretess).
- **Privacy by design:** Rekommendation att använda svenska/EU-baserade modeller som förstahandsval.
- **Påminnelser i plattformen:** Informationstexter påminner användare om begränsningarna.
- **Förvaltningsplan:** Reglerar roller, ansvar och rutiner för support och uppföljning.

3. Utbildning och medvetenhet:

- **Introduktionsutbildning:** Medarbetare som får tillgång till Intric genomgår:
- Basutbildning i AI
- Instruktionsfilmer
- Utbildningsmaterial om dataskydd och informationssäkerhet

- Ansvarsfull användning av AI-verktyg enligt kommunens riktlinjer
- **Återkommande information:** Påminnelser och information om säker användning publiceras på intranätet och via e-post.
- **Förvaltningsorganisation:** Enligt förvaltningsplanen ansvarar systemförvaltare för att identifiera och genomföra utbildningsinsatser riktade till systemadministratörer och funktionsansvariga.

4. Behörighetsstyrning:

- **Princip om minsta behörighet:** Endast medarbetare som har ett faktiskt behov får tillgång till Intric-plattformen.
- **Rollbaserad åtkomst:** Systemadministratörer per sektor hanterar behörigheter och konton inom den egna sektorn enligt förvaltningsplanen.
- **Regelbunden översyn:** Behörigheter ses över minst årligen (halvårsvis enligt INFORMATIONSSÄKERHETSKRAV Access Review) och användarkonton för medarbetare som slutat avskiljs omgående enligt kommunens offboarding-rutiner (Offboarding Checklist).

5. Incidenthantering:

- **Rutiner för rapportering:** Medarbetare instrueras att omgående rapportera misstänkta säkerhetsincidenter eller avvikelser enligt kommunens rutiner för incidentrapportering för informationssäkerhet och dataskydd.
- **Support och eskalering:** Systemadministratörer och funktionsansvariga hanterar första linjens support och eskalerar vid behov enligt förvaltningsplanen.
- **Anmälningsplikt:** Vid personuppgiftsincident som innebär risk för registrerades fri- och rättigheter, anmäler kommunen till Integritetsskyddsmyndigheten inom 72 timmar enligt artikel 33 GDPR.
- **Information till registrerade:** Vid allvarlig incident informeras berörda registrerade enligt artikel 34 GDPR.
- **Intricsincidenthantering:** Intric AB har dokumenterade rutiner för övervakning, upptäckt, analys, rapportering, eskalering och hantering av säkerhetshändelser och incidenter enligt Incident Response Plan med Post-Incident Review inom 30 dagar.

6. Verksamhetskontinuitet:

- **Backup och återställning:** Säkerhetskopiering säkerställer att data kan återställas vid tekniskt fel eller incident.
- **Business Continuity Plan (BCP):** Intric har en dokumenterad BCP med roller, kommunikationskedjor och Disaster Recovery Plan (DRP).
- **Multi-zone deployment:** Automatiskt failover och load balancing samt regelbundna DR-tester.
- **Alternativa arbetssätt:** Medarbetare kan fortsätta sitt arbete med andra metoder om Intric-plattformen blir otillgänglig.

7. Avtal och ansvarsfördelning:

- **Tydliga roller:** PUB-avtalet definierar tydligt vem som ansvarar för vilka säkerhetsåtgärder (kommunen vs. Intric AB).
- **Förvaltningsorganisation:** Förvaltningsplanen reglerar roller och ansvar inom kommunen, inklusive systemägare, systemförvaltare, systemadministratörer per sektor, förvaltningsgrupp och funktionsansvariga.
- **Revisionsrättigheter:** Kommunen har rätt att granska Intricsoch Glesys säkerhetsarbete genom auditering eller certifieringsrapporter. Intric AB har godkänt Audit Right Clause i kontraktet för årlig audit.

8. Certifieringar och standarder:

- **ISO/IEC 27001:2022:** Intric AB har certifiering enligt ISO/IEC 27001:2022 (certifikat ACCISMS2025110188), vilket bekräftar ett fullständigt implementerat och certifierat ledningssystem för informationssäkerhet.
- **Informationssäkerhetsnivå 3-3-3:** Fullständig bedömning visar att Intric uppfyller alla 93 krav för säkerhetsnivå 3 (konfidentialitet, riktighet, tillgänglighet).
- **Omfattande säkerhetsramverk:** Intrics ISMS omfattar dokumenterade policyer för Access Control, Baseline Hardening, Change Management, Vendor Management, Threat Intelligence, Risk Management, Data Protection, Privacy Policy, Backup Policy, Incident Response och många fler områden.
- **Glesys säkerhetsstandarder:** Glesys driver datacenter med hög säkerhetsnivå i Sverige.

9. Intern kontroll och uppföljning:

- **Säkerhetsöversyn:** Systemförvaltaren och dataskyddsombud genomför regelbundna översyner av säkerhetsåtgärderna.
- **Riskbedömningar:** Vid förändringar i systemet eller verksamheten genomförs nya riskbedömningar.

10. Särskilda åtgärder för tredjelandsöverföringar:

För AI-modeller som driftas i USA (OpenAI, Anthropic):

- **Minimering av dataöverföring:** Endast kontext (prompter) delas, inte användaridentifierande information.
- **Användarval:** Användare väljer aktivt vilken modell de vill använda och kan välja svenska eller europeiska alternativ (Managed by Intric, Llama 3.3 SWE, Mistral) om de föredrar det.
- **Rekommendation:** Privacy by design-principen implementeras genom rekommendation av svenska/EU-baserade modeller som förstahandsval.
- **Standardavtalsklausuler (SCC):** Överföringen skyddas av SCC då OpenAI och Anthropic inte är certifierade enligt EU-U.S. Data Privacy Framework.
- **Se avsnitt 4.4** för fullständig genomgång av tredjelandsöverföringar och skyddsåtgärder.

Sammanfattning – Integritet och konfidentialitet:

Omfattande tekniska och organisatoriska säkerhetsåtgärder säkerställer att personuppgifter skyddas mot obehörig åtkomst, förlust eller skada. Kryptering, åtkomstkontroll, loggning, säkerhetskopiering, utbildning, riktlinjer och tydlig ansvarsfördelning skapar tillsammans en hög säkerhetsnivå. Certifieringar (ISO 27001:2022, INFORMATIONSSÄKERHETSKRAV 3-3-3) och avtal med leverantörer stärker förtroendet för att säkerhetsåtgärderna upprätthålls kontinuerligt. Privacy by design-principen implementeras genom rekommendation av svenska/EU-baserade modeller.

Verifiering av informationssäkerhetsnivå 3-3-3:

Intric AB har genomgått en fullständig bedömning enligt INFORMATIONSSÄKERHETSKRAV-ramverket och uppfyller samtliga 93 krav för säkerhetsnivå 3 inom konfidentialitet, riktighet och tillgänglighet.

Sammanfattning av verifierade säkerhetsåtgärder:

Ledningssystem och organisation:

- ISO 27001:2022-certifierat ISMS (certifikat ACCISMS2025110188) med årlig granskning
- Dokumenterade roller och ansvar i ISMS-manual och Statement of Applicability
- Segregation of Duties (SoD) genom tekniska och organisatoriska åtskillnader
- Tydlig ansvarskedja från ledning till operativ nivå

Tillgångshantering och åtkomstkontroll:

- Asset Register med dokumenterade ägare och ansvar
- Rollbaserad åtkomstkontroll (RBAC) med halvårsvisa Access Review-processer
- Identity Management med unika, personliga ID:n och spårbar historik
- Privileged Account Management med separata administratörskonton, MFA och session recording
- Password Policy med komplexitetskrav och godkända lösenordshanteringsverktyg
- Offboarding Checklist med automatisk radering och återlämnande av tillgångar

Teknisk säkerhet:

- SSL/TLS-kryptering för all kommunikation
- AES-256-kryptering för flyttbar media
- Key Management Policy med HSM för nyckelgenerering och rotation varje år
- Endpoint Protection Platform med realtids antivirus och heuristik
- Vulnerability Management med månatlig scanning, CVSS-baserad prioritering och årlig penetrationstest
- Configuration Management Database (CMDB) med baselines och avvikelseteknik
- Data Loss Prevention (DLP)-lösning över e-post, cloud-lagring och endpoints

- Multi-factor Authentication (MFA) obligatorisk för alla administrativa konton

Övervakning och incidenthantering:

- SIEM-system samlar loggar från alla system i write-once storage
- Continuous Monitoring med anomaly detection i nätverk och applikationer
- Threat Intelligence Process via Security Operations Center (SOC)
- Incident Response Plan med detection, analys, eskalering och kommunikation till beställare
- Post-Incident Review dokumenteras inom 30 dagar
- Security Incident Ticket-system med automatiska notifieringar

Backup och kontinuitet:

- Backup Policy med dagliga inkrementella backups, veckovisa fulla backups
- Säkerhetskopior lagras i separerad Availability Zone, krypterade
- Kvartalsvis testning av återställning
- Business Continuity Plan (BCP) med roller, kommunikationskedjor och DRP
- Multi-zone deployment med automatiskt failover och load balancing
- Regelbundna DR-tester

Fysisk säkerhet:

- Datacenter med åtkomstkontroll via badge-system och CCTV
- Skyddsnivå enligt MSB 629 för IT-utrymmen
- Endast behörig personal med bakgrundskontroll får tillträde
- UPS-system och generatorbackup för kritiska serverhallar
- Clean Desk Policy och automatisk låsning av arbetsstationer efter 5 minuter

Säker utveckling och ändringshantering:

- Secure SDLC med Threat Modeling, SAST/DAST, code review och pentest
- Security Requirements Traceability Matrix
- Coding Standards (OWASP Top 10) integrerade i CI-pipeline
- Change Management Process med risk assessment, godkännande och rollback-plan
- Separation av utvecklings-, test- och produktionsmiljöer (VPC/subnets)

Personal och kompetens:

- Bakgrundskontroll av personal innan anställning
- Security Awareness Programme med årlig e-learning och phishing-simuleringar
- Alla anställda undertecknar Non-Disclosure Agreement (NDA)

- Disciplinary Policy för överträdelser
- Exit Procedure med signering av ansvarsförbindelse

Leverantörskedja:

- Supply Chain Security Policy med säkerhetsbedömning av underleverantörer
- Vendor Management Policy med kontaktperson för regulatoriska myndigheter
- Lista över godkända underleverantörer delas med beställaren
- Audit Right Clause i kontrakt för årlig audit av beställaren

Regelefterlevnad:

- Compliance Management Process för löpande laguppföljning
- Privacy Policy och Secure Development Guidelines med privacy-by-design
- GDPR-kontroller implementerade med DPO-roller och utbildning
- Media Sanitization enligt NIST 800-88
- Secure Deletion Procedure enligt DoD-standard
- Time Sync mot svenska NTP-servrar (UTC(SP))

Sammanfattande bedömning från INFORMATIONSSÄKERHETSKRAV-analysen:

"Leverantören uppfyller samtliga krav för säkerhetsnivå 3-3-3 i enlighet med de levererade dokumenten. Ingen kritisk brist har identifierats. Alla kontroller är spårbara, regelbundet granskade och förenliga med nivå 3-kraven."

Denna omfattande verifiering genom INFORMATIONSSÄKERHETSKRAV-ramverket bekräftar att Intric AB har implementerat och upprätthåller en säkerhetsnivå som motsvarar höga krav på konfidentialitet, riktighet och tillgänglighet, vilket är särskilt viktigt för kommunala verksamheter som behandlar personuppgifter och annan skyddsvärd information.

4.3 Registrerades rättigheter

De registrerade har ett antal rättigheter enligt kapitel III i dataskyddsförordningen. Kommunen ska säkerställa att dessa rättigheter kan tillgodoses.

Rätten till information (artiklarna 12–14 GDPR)

Åtgärder:

Medarbetare informeras om behandlingen enligt beskrivningen under "Principen om laglighet, korrekthet och öppenhet" (avsnitt 4.2). Information lämnas vid onboarding, via intranät och genom utbildning.

Externa personer vars uppgifter kan förekomma i användarinteraktioner informeras genom kommunens allmänna integritetspolicy på webbplatsen.

Rätten till tillgång (artikel 15 GDPR)

Registrerades rätt:

Den registrerade har rätt att få bekräftelse på om personuppgifter som rör hen behandlas, och i så fall få tillgång till uppgifterna samt information om behandlingen.

Åtgärder:

För medarbetare:

- Medarbetare kan vända sig till systemförvaltaren för att begära ut sina personuppgifter från Intric-plattformen. Om den personuppgiftsansvarige inte lämnar ut uppgifterna kan den registrerade därefter kontakta dataskyddsombudet.
- Systemförvaltaren kan extrahera användaruppgifter (namn, e-post, användar-ID), loggdata och konversationshistorik kopplad till användarens konto.
- Informationen lämnas ut inom en månad enligt artikel 12.3 GDPR.

För externa personer:

- Om en extern person begär ut sina personuppgifter från kommunen och uppgifterna kan finnas i Intric, genomför Systemförvaltaren en sökning i konversationshistorik kopplad till relevanta användarkonton.
- Om uppgifterna finns, lämnas de ut tillsammans med information om behandlingen.

Utmaning: Eftersom AI-modelleverantörer (OpenAI, Anthropic, Mistral) behandlar kontext (prompter) men inte lagrar koppling till enskilda kommunala användare, kan det vara svårt att identifiera vilka uppgifter om en extern person som har behandlats av dessa leverantörer. Kommunen kan dock lämna ut information om vilka uppgifter som har inkluderats i prompter inom Intric-plattformen.

Rätten till rättelse (artikel 16 GDPR)

Registrerades rätt:

Den registrerade har rätt att utan onödigt dröjsmål få felaktiga personuppgifter rättade.

Åtgärder:

För medarbetare:

- Medarbetare kan begära rättelse av sina användaruppgifter (t.ex. vid namnbyte eller byte av e-postadress) genom att kontakta Systemförvaltaren.
- Systemförvaltaren rättar uppgifterna i Intric-plattformen och, om tillämpligt, i källsystemet (HR-system, Active Directory) för att säkerställa att uppgifterna förblir korrekta.

För externa personer:

- Om en extern person begär rättelse av uppgifter som förekommer i en tidigare sparad konversation i Intric, kan Systemförvaltaren uppdatera eller radera den aktuella konversationen.

- Användare instrueras att vara noggranna med att använda korrekta uppgifter när de inkluderar personuppgifter i prompter.

Rätten till radering (artikel 17 GDPR)

Registrerades rätt:

Den registrerade har under vissa omständigheter rätt att få sina personuppgifter raderade utan onödigt dröjsmål.

Åtgärder:

För medarbetare:

- Medarbetare kan begära radering av sina personuppgifter när användarkontot avslutas.
- Personuppgifter raderas automatiskt enligt fastställda lagringstider (se avsnitt om lagringsminimering).
- Konversationshistorik kan raderas på begäran av användaren innan lagringstiden löper ut.

Begränsningar:

- Om radering skulle hindra kommunen från att fullgöra en rättslig förpliktelse (t.ex. bevara loggdata för säkerhetsändamål enligt informationssäkerhetspolicy) kan begäran avslås med motivering.

För externa personer:

- Om en extern person begär radering av uppgifter som förekommer i en sparad konversation i Intric, raderas konversationen om det inte finns lagstadgade skäl att bevara den.

Utmaning för data hos AI-modelleverantörer:

- Eftersom endast kontext (ej användaridentifierande information) delas med AI-modelleverantörer, och dessa uppgifter inte är direkt spårbara till en specifik person, kan det vara tekniskt svårt att radera uppgifter hos dessa leverantörer.
- Kommunen informerar registrerade om denna begränsning i sin integritetspolicy.

Rätten till begränsning av behandling (artikel 18 GDPR)

Registrerades rätt:

Den registrerade har rätt att begära att behandlingen begränsas under vissa omständigheter (t.ex. om riktigheten av uppgifterna bestrids).

Åtgärder:

- Om en medarbetare begär begränsning av behandlingen kan systemförvaltaren tillfälligt spärra användarens konto eller flagga uppgifterna som "under översyn" tills frågan är utredd.
- Under tiden behandlingen är begränsad får uppgifterna endast lagras, inte användas för andra ändamål.

Rätten till dataportabilitet (artikel 20 GDPR)

Registrerades rätt:

Den registrerade har rätt att få ut sina personuppgifter i ett strukturerat, allmänt använt och maskinläsbart format och rätt att överföra uppgifterna till en annan personuppgiftsansvarig.

Tillämpbarhet:

Dataportabilitet gäller endast när behandlingen grundas på samtycke eller avtal och sker automatiserat. Eftersom behandlingen i Intric grundas på uppgift av allmänt intresse (artikel 6.1 e GDPR), är dataportabilitet normalt inte tillämplig.

Åtgärder vid tillämpliga fall:

Om rätten är tillämplig kan Systemförvaltaren exportera användarens personuppgifter (användaruppgifter, konversationshistorik) i ett strukturerat format (t.ex. JSON eller CSV) och lämna ut till den registrerade.

Rätten att göra invändningar (artikel 21 GDPR)

Registrerades rätt:

Den registrerade har rätt att invända mot behandling som grundas på uppgift av allmänt intresse (artikel 6.1 e) eller myndighetsutövning. I detta fall grundas behandlingen på artikel 6.1 e.

Åtgärder:

För medarbetare:

- En medarbetare kan invända mot att dennes personuppgifter behandlas i Intric-plattformen.
- Kommunen prövar invändningen och upphör med behandlingen, om inte kommunen kan visa tvingande berättigade skäl som väger tyngre än den registrerades intressen, rättigheter och friheter, eller om behandlingen är nödvändig för fastställande, utövande eller försvar av rättsliga anspråk.
- I praktiken innebär det att medarbetarens användarkonto avskiljs och personuppgifter raderas.

För externa personer:

- En extern person kan invända mot att dennes uppgifter behandlas i Intric.
- Kommunen prövar invändningen och kan vidta åtgärder som att radera konversationer där personens uppgifter förekommer, eller instruera medarbetare att inte inkludera personens uppgifter i framtida användning.

Rätten att inte bli föremål för automatiserat beslutsfattande (artikel 22 GDPR)

Tillämpbarhet:

Intric-plattformen används **INTE** för att fatta automatiserade beslut som har rättsliga följder för eller på liknande sätt i betydande grad påverkar en fysisk person.

AI-modellerna används endast som stöd för textproduktion, analys och administration. Beslut fattas alltid av mänskliga medarbetare, inte av AI-systemet självt.

Åtgärder:

Kommunens Riktlinjer för artificiell intelligens (AI) tydliggör att:

- "Inom kommunkoncernen får AI inte användas för automatiserat beslutsfattande utan att mänsklig kontroll sker av det som AI genererat eller bidragit till."
- "Som medarbetare är du ansvarig för de resultat som genereras eller skapas och för de beslut som bereds eller tas med stöd av AI"
- "Vid beslut som påverkar enskilda, där AI har använts som stöd, ska det alltid vara en människa med delegerat ansvar som kontrollerar och fattar det slutliga beslutet."

Medarbetare får inte blint förlita sig på AI-genererade svar.

Rutiner för att tillgodose registrerades rättigheter

- **Kontaktvägar:** Tydliga kontaktuppgifter till Systemförvaltaren och dataskyddsombud finns tillgängliga på intranätet och webbplatsen.
- **Formulär:** Ett webbformulär eller e-postadress för registrerade att begära utövande av sina rättigheter.
- **Hanteringsprocess:** Systemförvaltaren har en process för att ta emot, registrera och handlägga begäranden från registrerade.
- **Svarstid:** Begäranden besvaras inom en månad enligt artikel 12.3 GDPR. Vid komplexa ärenden kan tiden förlängas med ytterligare två månader med motivering.
- **Dokumentation:** Alla begäranden och åtgärder dokumenteras för att visa efterlevnad.

Sammanfattning – Registrerades rättigheter:

Kommunen har etablerat rutiner och processer för att säkerställa att registrerades rättigheter kan tillgodoses. Information lämnas proaktivt, och registrerade har tydliga kontaktvägar för att utöva sina rättigheter. Tekniska möjligheter finns för att extrahera, rätta och radera personuppgifter vid behov. Begränsningar som följer av rättsliga skyldigheter eller tekniska förutsättningar kommuniceras tydligt.

Praktiska begränsningar (förtydligande efter DSO:s yttrande)

Dataskyddsombudet har påpekat att det finns praktiska svårigheter att identifiera externa personers uppgifter i prompter, särskilt om konversationer är många och ostrukturerade. Följande faktiska begränsningar förtydligas:

– Prompter är fritextfält och strukturerade sökningar kan vara begränsade. Det kan vara svårt att hitta alla förekomster av en specifik persons uppgifter.

– Eftersom endast kontext (ej användaridentifierande information) delas med AI-modelleverantörer, och dessa uppgifter inte är direkt spårbara, är det tekniskt svårt att begära radering av specifika uppgifter hos OpenAI och Anthropic.

– Enligt dokumenterade DPA:er raderas data automatiskt efter max 30 dagar hos dessa leverantörer, vilket begränsar exponeringstiden.

Kommunens åtgärder: Proaktiv information via integritetspolicy om att personuppgifter kan förekomma i digitala verktyg. Kort lagringstid minimerar exponering. Vid begäran genomförs rimliga åtgärder för att identifiera och radera uppgifter i Intric-plattformen (best effort). Kommunen informerar om att radering hos amerikanska leverantörer är tekniskt begränsad men att automatisk radering sker efter 30 dagar.

4.4 Skyddsåtgärder för internationella överföringar

Översikt

Behandlingen i Intric-plattformen innebär överföringar av personuppgifter till tredjeland (USA) när användare väljer att använda AI-modeller från OpenAI eller Anthropic. Denna behandling kräver särskilda skyddsåtgärder enligt kapitel V i dataskyddsförordningen.

När sker tredjelandsöverföring?

Tredjelandsöverföring sker endast när:

Användare aktivt väljer att använda en AI-modell från OpenAI (GPT-modeller) eller Anthropic (Claude-modeller). Då överförs kontexten (prompten och eventuellt bifogade filer) samt IP-adressen från Intricsserver till dessa företags servrar i [redacted]

Vilken information överförs:

- Kontext (prompter och bifogade filer) som kan innehålla personuppgifter om externa personer (namn, e-post, telefonnummer)
- IP-adress från Intricsserver (inte användarens IP-adress)

Vilken information överförs INTE:

- Användarens namn
- Användarens e-postadress
- Användar-ID

Denna minimering av dataöverföring är en viktig skyddsåtgärd som minskar risken för registrerades integritet.

Bedömning av [redacted] Data Privacy Framework

VIKTIGT: OpenAI och Anthropic är inte certifierade enligt EU-U.S. Data Privacy Framework (DPF).

Enligt information från Privacy Shield Framework (www.dataprivacyframework.gov) (Senast kollad 2025-12-12) är varken OpenAI eller Anthropic listade som certifierade företag enligt det EU-amerikanska dataskyddsramverket som trädde i kraft 2023.

Konsekvenser av att DPF inte är tillämpligt:

1. **Ingen adekvansgrund:** Kommunen kan inte stödja sig på EU-kommissionens beslut om adekvat skyddsnivå för överföringen till dessa leverantörer.
2. **Krav på alternativa skyddsåtgärder:** Överföringen måste istället skyddas av andra mekanismer enligt artikel 46 GDPR, främst standardavtalsklausuler (SCC).
3. **Högre riskbedömning:** Frånvaron av DPF-certifiering innebär att den personuppgiftsansvarige har mindre garantier för skyddsnivån och begränsad möjlighet till klagomål och rättsmedel för de registrerade.
4. **Risk för US CLOUD Act:** Amerikanska myndigheter kan enligt US CLOUD Act begära tillgång till data som lagras av amerikanska företag, även om data lagras utanför USA. Detta kan inte undvikas genom SCC.

Skyddsåtgärder som vidtas

Trots att OpenAI och Anthropic inte är DPF-certifierade bedöms överföringen kunna ske under förutsättning att följande skyddsåtgärder är på plats:

1. Standardavtalsklausuler (SCC)

Beskrivning:

Intric AB har tecknat formella Data Processing Agreements med OpenAI och Anthropic som inkluderar EU-kommissionens standardavtalsklausuler (SCC) enligt artikel 46.2 c GDPR:

OpenAI:

- **Data Processing Addendum** daterat 24 januari 2024 (undertecknat av Intric AB 8 maj 2025)
- **SCC Module Two** (Controller to Processor) appliceras
- Baseras på EU-kommissionens beslut från 4 juni 2021
- Governing law: England and Wales (Clause 17)
- Disputes: Courts of England and Wales (Clause 18)

Anthropic:

- **Data Processing Addendum** ikraftträdande 24 februari 2025
- **SCC Module Two** (Controller to Processor) och **Module Three** (Processor to Sub-Processor) appliceras
- Governing law: Republic of Ireland (Clause 17)

- Disputes: Republic of Ireland (Clause 18)

Kommunens ansvar:

Personuppgiftsansvariga har via Intric AB säkerställt att giltiga SCC finns på plats med AI-modelleverantörerna och att dessa SCC är korrekt implementerade med lämpliga moduler och annexer.

Begränsningar med SCC:

SCC ger avtalsrättsliga garantier, men kan inte förhindra att amerikanska myndigheter begär åtkomst till data enligt amerikansk lagstiftning (t.ex. CLOUD Act, FISA 702). Därför krävs kompletterande åtgärder.

2. Minimering av dataöverföring

Beskrivning:

Endast kontext (prompter och bifogade filer) och Intric server-IP överförs till AI-modelleverantörerna. Ingen användaridentifierande information (namn, e-post, användar-ID) delas. Detta innebär att:

- Det inte finns någon direkt koppling mellan en enskild kommunanställd och data som behandlas av OpenAI/Anthropic.
- Risken för integritetsintrång minskar avsevärt, eftersom leverantörerna inte kan identifiera vem som har skickat en viss prompt.

Juridisk betydelse:

Denna minimering av dataöverföring är en av de mest effektiva tekniska åtgärderna för att minska riskerna vid tredjelandsöverföringar. Det faktum att endast kontext delas (inte metadata om användaren) gör att även om amerikanska myndigheter skulle begära tillgång till data, kan de inte enkelt koppla detta till specifika individer i Lidköpings kommun.

3. Användarval och alternativ

Beskrivning:

Kommunen har implementerat en "privacy by design"-strategi där:

- Svenska/EU-baserade modeller (Managed by Intric, Llama 3.3 SWE, Mistral) rekommenderas som förstahandsval för arbetsuppgifter som kan innehålla personuppgifter.
- Användare informeras tydligt om vilka modeller som behandlar data i Sverige/EU respektive USA.
- Användare gör ett aktivt val när de väljer en amerikansk modell och är därmed medvetna om att överföring till USA sker.

Juridisk betydelse:

Genom att ge användare möjlighet att välja EU-baserade alternativ minimerar kommunen faktiskt antalet tredjelandsöverföringar. Detta är en form av frivillig riskreducering som visar på ansvarsfull hantering.

4. Förbud mot känsliga personuppgifter och sekretess

Beskrivning:

Kommunens riktlinjer förbjuder explicit att:

- Känsliga personuppgifter enligt artikel 9 GDPR behandlas i Intric
- Sekretessbelagd information enligt offentlighets- och sekretesslagen hanteras
- Uppgifter om underåriga barn inkluderas

Dessa förbud gäller oavsett vilken modell som används, men är särskilt viktiga vid tredjelandsöverföringar.

Juridisk betydelse:

Genom att begränsa vilken typ av personuppgifter som får överföras till USA minskar kommunen allvarlighetsgraden av eventuella risker. Endast grundläggande kontaktuppgifter (namn, e-post, telefonnummer) kan i praktiken överföras, vilket innebär att konsekvenserna av obehörig åtkomst är begränsade.

5. Utbildning och användaransvar

Beskrivning:

Alla användare genomgår:

- Basutbildning i AI
- Instruktionsfilmer om dataskydd
- Genomgång av kommunens riktlinjer
- Påminnelser i användargränssnittet

Juridisk betydelse:

Användare är medvetna om riskerna och tar ett informerat beslut när de väljer amerikanska modeller. De är också instruerade att minimera vilka personuppgifter som inkluderas i prompter.

6. Kontraktuella åtaganden från leverantörerna

Beskrivning:

Enligt dokumenterade Data Processing Agreements med OpenAI och Anthropic:

OpenAI DPA (daterat 24 januari 2024):

- Data används **inte** för att träna AI-modeller
- API Service data lagras i **max 30 dagar**, därefter automatisk radering
- ChatGPT Enterprise data lagras under avtalstiden

- **Säkerhetscertifieringar:** SOC 2 Type II
- **Säkerhetsåtgärder:** Kryptering (SSL/TLS, AES-256), MFA, RBAC, loggning, incidenthantering
- OpenAI ansvarar för sina subprocessors handlingar
- Customer data behandlas endast enligt instruktioner från Customer

Anthropic DPA (ikraftträdande 24 februari 2025):

- Data "säljs" eller "delas" **inte** enligt US Privacy Laws
- Data lagras i **30 dagar efter avtalets upphörande**, därefter radering
- **Säkerhetscertifieringar:** SOC 2, penetrationstestning årligen
- **Säkerhetsåtgärder:** AES-256 kryptering, TLS 1.2+, MFA, EDR, SIEM/SOAR, incidenthantering
- Data används endast för att tillhandahålla tjänsten
- Anthropic ansvarar för sina subprocessors handlingar

Juridisk betydelse:

Dessa kontraktuella åtaganden är juridiskt bindande och ger kommunen avtalsrättsliga garantier för hur data behandlas. DPA:erna specificerar säkerhetsåtgärder, lagringstider och förbud mot vidareutnyttjande, vilket reducerar riskerna avsevärt jämfört med att enbart förlita sig på leverantörernas policyer.

Riskbedömning för tredjelandsöverföringar

Identifierade risker:

A) Risk för myndighetstillgång enligt US CLOUD Act och FISA 702

Amerikanska säkerhets- och underrättelsetjänster kan enligt amerikansk lagstiftning begära tillgång till data som lagras eller behandlas av amerikanska företag, även om dessa har datacenter utanför USA.

Sannolikhet: Låg till Medel

- För allmänna administrativa prompter (projektplaner, textmallar) är sannolikheten för att amerikanska myndigheter skulle ha intresse av att begära åtkomst mycket låg.
- Om prompter skulle innehålla information som kan vara av säkerhetsintresse (vilket de inte ska enligt riktlinjerna) ökar sannolikheten.

Allvarlighetsgrad: Relativt allvarliga

- Eftersom endast kontext (inte användaridentifierande information) delas, och känsliga uppgifter är förbjudna, är konsekvenserna begränsade.
- Det faktum att OpenAI och Anthropic inte är DPF-certifierade innebär dock att registrerade har sämre rättsmedel och möjlighet till klagomål.

Mitigering:

- Endast grundläggande kontaktuppgifter får behandlas
- Användaridentifierande information delas inte
- Användare kan välja EU-alternativ
- Förbud mot känsliga uppgifter och sekretess

B) Bristande insyn och kontroll

Kommunen har begränsad möjlighet att kontrollera hur OpenAI och Anthropic faktiskt hanterar data internt, hur länge prompter lagras och vilka säkerhetsåtgärder som faktiskt är på plats.

Sannolikhet: Medel

- Det är svårt att verifiera leverantörernas faktiska efterlevnad utan direktaudit.

Allvarlighetsgrad: Begränsade till Relativt allvarliga

- Risken begränsas av att endast kontext delas och känsliga uppgifter är förbjudna.

Mitigering:

- Standardavtalsklausuler ger vissa kontraktuella garantier
- Användare kan välja EU-alternativ
- Kontinuerlig bevakning av leverantörernas policyer och certifieringar

C) Framtida förändringar i rättsläge

Det finns risk för att rättsläget förändras på ett sätt som gör tredjelandsöverföringar till USA mer problematiska (t.ex. att EU-domstolen ogiltigförklarar SCC, eller att amerikanska övervakningslagar utökas).

Sannolikhet: Låg

- Historiskt har sådana förändringar varit förhållandevis sällsynta (Schrems I 2015, Schrems II 2020, DPF 2023).

Allvarlighetsgrad: Allvarliga

- Om överföringen plötsligt blir olaglig måste kommunen omgående upphöra med användningen av amerikanska modeller.

Mitigering:

- Kontinuerlig bevakning av rättsläge
- Alternativa EU-baserade modeller finns tillgängliga
- Beredskap att snabbt byta leverantör

Slutsats och sammantagen bedömning

Sammanfattande bedömning av tredjelandsöverföringar till USA:

Trots att OpenAI och Anthropic inte är certifierade enligt EU-U.S. Data Privacy Framework bedöms överföringen av kontext (prompter) till dessa leverantörer kunna ske under följande förutsättningar:

Uppfyllda förutsättningar:

1. **Standardavtalsklausuler (SCC) är på plats** via Intric AB
2. **Minimering av dataöverföring** – endast kontext delas, inte användaridentifierande information
3. **Privacy by design** – svenska/EU-modeller rekommenderas som förstahandsval
4. **Förbud mot känsliga personuppgifter och sekretess** minskar allvarlighetsgraden av risker
5. **Utbildning och informerade användarval** – användare väljer aktivt och är medvetna om överföringen
6. **Kontinuerlig uppföljning** – rättsläget bevakas och alternativa lösningar finns tillgängliga

Restrisker:

Kvarstående risker som inte kan elimineras:

- Risk för myndighetstillgång enligt US CLOUD Act (kan inte förhindras av SCC)
- Begränsad insyn och kontroll över leverantörernas faktiska hantering
- Beroende av att rättsläget inte förändras på ett sätt som ogiltigförklarar SCC

Dessa risker bedöms dock som **acceptabla** med hänsyn till:

- Den begränsade typen av personuppgifter som kan överföras (grundläggande kontaktuppgifter)
- Att överföringen sker frivilligt genom användarens aktiva val
- Att alternativa EU-baserade modeller finns tillgängliga
- Att omfattande utbildning och riktlinjer minimerar risken för felaktig användning

Rekommendation:

Kommunen rekommenderar starkt att användare väljer svenska/EU-baserade modeller (Managed by Intric, Llama 3.3 SWE, Mistral) som förstahandsval för arbetsuppgifter som kan innehålla personuppgifter. Detta i enlighet med principen om privacy by design och för att minimera tredjelandsöverföringar.

Användning av amerikanska modeller (OpenAI, Anthropic) tillåts endast när:

- Användaren har gjort ett aktivt och informerat val
- Kommunens riktlinjer följs (inga känsliga uppgifter, ingen sekretess)
- Det inte finns ett lämpligt EU-alternativ för den specifika arbetsuppgiften

Uppföljning:

Kommunen kommer att:

- Kontinuerligt bevaka rättsläget avseende tredjelandsöverföringar
- Följa utvecklingen av OpenAI och Anthropics certifieringar (t.ex. eventuell framtida DPF-certifiering)
- Utvärdera alternativa EU-baserade modeller löpande
- Vara beredd att omgående upphöra med användning av amerikanska modeller om rättsläget förändras

Se **avsnitt 5 (Riskhantering)** för detaljerad bedömning av risker R04 och R09 som specifikt rör tredjelandsöverföringar.

Transfer Impact Assessment (TIA)

I enlighet med dataskyddsombudets rekommendation har kommunen genomfört en formell Transfer Impact Assessment enligt EDPB:s riktlinjer för överföringar till USA (OpenAI och Anthropic).

Mottagare: OpenAI OpCo, LLC (USA) och Anthropic PBC (USA). Överföringsmekanism: SCC Module Two.

Uppgifter som överförs: Kontext (prompter och bifogade filer) som kan innehålla grundläggande kontaktuppgifter. INTE användaridentifierande information.

Analys av mottagarlandets lagstiftning: CLOUD Act och FISA 702 ger amerikanska myndigheter tillgång till data hos amerikanska företag. Executive Order 14086 har förbättrat skyddet men nivån bedöms inte som väsentligen likvärdig med EU.

Sannolikhetsbedömning: Sannolikheten för myndighetstillgång bedöms som låg. Prompterna innehåller generisk administrativ information utan koppling till säkerhetshotande verksamhet.

Kompletterande åtgärder: Kryptering (SSL/TLS), dataminimering (endast kontext delas), privacy by design-rekommendation, förbud mot känsliga uppgifter, utbildning, max 30 dagars lagring hos leverantörer.

Slutsats: Överföringar kan ske under förutsättning att SCC och kompletterande åtgärder är på plats, svenska/EU-modeller rekommenderas som förstahandsval, användare gör informerat val, och kontinuerlig bevakning av rättsläget genomförs.

Restrisker: Risk för myndighetstillgång (CLOUD Act) kan inte elimineras av SCC. Begränsade rättsmedel då leverantörerna inte är DPF-certifierade. Restriskerna bedöms som acceptabla med hänsyn till begränsade uppgiftstyper och aktiva användarval.

Fullständig TIA dokumenteras som separat bilaga och ses över årligen.

4.5 Sammantagen bedömning

Efter genomförd rättslig analys bedöms de rättsliga förutsättningarna för behandlingen som uppfyllda.

Sammanfattning:

1. Rättslig grund:

Behandlingen har tydlig och giltig rättslig grund:

- För medarbetares användaruppgifter: Uppgift av allmänt intresse (artikel 6.1 e GDPR)

2. Dataskyddsprinciper:

Samtliga grundläggande dataskyddsprinciper följs:

- Laglighet, korrekthet och öppenhet: Behandlingen har rättslig grund, är rättvis och transparent
- Ändamålsbegränsning: Tydligt definierade och avgränsade ändamål
- Uppgiftsminimering: Endast nödvändiga personuppgifter behandlas, privacy by design genom rekommendation av svenska/EU-modeller
- Riktighet: Åtgärder för att säkerställa korrekta uppgifter
- Lagringsminimering: Fastställda lagringstider och automatisk gallring
- Integritet och konfidentialitet: Omfattande tekniska och organisatoriska säkerhetsåtgärder (ISO 27001:2022, INFORMATIONSSÄKERHETSKRAV 3-3-3)

3. Registrerades rättigheter:

Rutiner och processer finns för att tillgodose registrerades rättigheter enligt GDPR kapitel III. Informationsansvar uppfylls genom proaktiv information och tydliga kontaktvägar.

4. Internationella överföringar:

Tredjelandsöverföringar till USA för AI-modeller från OpenAI och Anthropic sker endast när användare aktivt väljer dessa modeller. Överföringen skyddas av:

- Standardavtalsklausuler (SCC)
- Minimering av dataöverföring (endast kontext, inte användaridentifierande information)
- Privacy by design-rekommendation av svenska/EU-modeller
- Förbud mot känsliga uppgifter och sekretess
- Informerade användarval

Riskerna bedöms som acceptabla med beaktande av dessa skyddsåtgärder. Se avsnitt 4.4 för fullständig analys.

5. Nödvändighet och proportionalitet:

Behandlingen är **nödvändig** för att möjliggöra för kommunen att använda moderna AI-verktyg för att effektivisera sitt arbete och höja kvaliteten i kommunikation och service till invånare. De specificerade ändamålen är noga avgränsade till områden där känsliga personuppgifter och sekretess inte förekommer.

Behandlingen är **proportionerlig** eftersom:

- Endast grundläggande identitetsuppgifter om medarbetare behandlas för plattformsadministration

- Personuppgifter om externa personer som kan förekomma i användarinteraktioner är begränsade till grundläggande kontaktuppgifter
- Tydliga riktlinjer och tekniska varningar förhindrar att känsliga uppgifter eller sekretess hanteras
- Omfattande säkerhetsåtgärder minimerar riskerna (ISO 27001:2022, INFORMATIONSSÄKERHETSKRAV 3-3-3)
- Privacy by design-principen implementeras genom rekommendation av svenska/EU-modeller
- Alternativa metoder (manuell textproduktion, externa konsulter) skulle vara betydligt mer kostsamma och tidskrävande

6. Gällande regelverk:

Behandlingen följer GDPR, svensk dataskyddslagstiftning, offentlighets- och sekretesslagen samt kommunens interna styrdokument. Leverantörer har relevanta certifieringar (ISO 27001:2022, INFORMATIONSSÄKERHETSKRAV 3-3-3) som stärker förtroendet.

Slutsats:

De rättsliga förutsättningarna för att genomföra behandlingen bedöms som uppfyllda. Behandlingen är laglig, nödvändig och proportionerlig. Behandlingen grundas primärt på artikel 6.1 e GDPR (uppgift av allmänt intresse) med stöd i kommunallagen (2017:725). Under förutsättning att fastställda riktlinjer, säkerhetsåtgärder och uppföljningsrutiner följs, kan behandlingen genomföras i enlighet med dataskyddsförordningen och kompletterande lagstiftning.

Steg 5. Riskhantering

Riskhanteringen för användningen av Intric-plattformen har genomförts med stöd av IMY:s Excelblad "Riskhantering vid konsekvensbedömning".

Metod

1. Identifiering av risker: Potentiella risker för enskildas fri- och rättigheter har identifierats genom workshops med IT-personal, dataskyddsombud och verksamhetsrepresentanter.

2. Analys av risker: Varje identifierad risk har bedömts utifrån:

- **Sannolikhet:** Hur troligt är det att risken inträffar? (Låg, Medel, Hög, Mycket hög)
- **Allvarlighetsgrad:** Hur allvarliga skulle konsekvenserna vara för enskilda om risken inträffar? (Begränsade, Relativt allvarliga, Allvarliga, Mycket allvarliga)

3. Riskreducerande åtgärder: För varje identifierad risk har åtgärder identifierats för att reducera sannolikheten och/eller allvarlighetsgraden.

4. Uppföljning: Efter att åtgärderna har beaktats har riskerna bedömts på nytt för att avgöra om kvarvarande risker är acceptabla.

Dokumentation

Den detaljerade riskhanteringen finns dokumenterad i bifogat Excelblad (se bilaga).

Sammanfattning av identifierade risker och åtgärder

Risk-ID	Identifierad risk	Sannolikhet (innan åtgärd)	Allvarlighetsgrad (innan åtgärd)	Riskreducerande åtgärder	Sannolikhet (efter åtgärd)	Allvarlighetsgrad (efter åtgärd)	Kvarvarande risk
[redacted]							

Risk-ID	Identifierad risk	Sannolikhet (innan åtgärd)	Allvarlighetsgrad (innan åtgärd)	Riskreducerande åtgärder	Sannolikhet (efter åtgärd)	Allvarlighetsgrad (efter åtgärd)	Kvarvarande risk
[redacted]							

Risk-ID	Identifierad risk	Sannolikhet (innan åtgärd)	Allvarlighetsgrad (innan åtgärd)	Riskreducerande åtgärder	Sannolikhet (efter åtgärd)	Allvarlighetsgrad (efter åtgärd)	Kvarvarande risk
[redacted]							

Risk-ID	Identifierad risk	Sannolikhet (innan åtgärd)	Allvarlighetsgrad (innan åtgärd)	Riskreducerande åtgärder	Sannolikhet (efter åtgärd)	Allvarlighetsgrad (efter åtgärd)	Kvarvarande risk
[redacted]							

Bedömning efter riskhantering

Samtliga identifierade risker har bedömts och riskreducerande åtgärder har identifierats. Efter beaktande av åtgärderna bedöms de kvarstående riskerna som **acceptabla**. Ingen risk bedöms längre som hög efter att åtgärderna har implementerats.

Särskilda förbehåll:

[redacted]

Förhandssamråd med IMY

Eftersom inga höga risker kvarstår efter implementering av riskreducerande åtgärder, föreligger **ingen skyldighet** att begära förhandssamråd med Integritetsskyddsmyndigheten enligt artikel 36 GDPR.

Förtydligande av risker tillagda efter DSO:s yttrande

Risk R12: Ändamålsglidning över tid. Plattformen införs brett och har många användningsområden.
[redacted]

Sannolikhet: Medel. Konsekvens: Allvarliga.

Riskreducerande åtgärder: Tydliga riktlinjer med [redacted]

Risk R13: Felaktig information från AI-modeller. AI-modeller kan generera felaktig information som ser korrekt ut. [redacted]

Sannolikhet: Medel till Hög. Konsekvens: Relativt allvarliga.

Riskreducerande åtgärder: [redacted]

Steg 6. Bedömning av skyldigheten att begära förhandssamråd

Efter att de riskreducerande åtgärderna har identifierats och integrerats i den planerade behandlingen kvarstår endast låga eller acceptabla risker. De risker som initialt bedömdes som potentiellt [redacted] reducerats till en nivå där de inte längre

utgör en hög risk för de registrerades rättigheter och friheter. Även de risker som identifierats efter DSO:s yttrande [redacted] bedöms som acceptabla efter åtgärder.

Bedömning

Behandlingen uppfyller därmed inte kriterierna för förhandssamråd enligt artikel 36 i dataskyddsförordningen. Ett förhandssamråd med Integritetsskyddsmyndigheten (IMY) bedöms därför **inte vara nödvändigt**.

Skäl till bedömningen

1. Omfattande riskreducerande åtgärder:

[redacted]

2. Minimerad databehandling:

- Endast grundläggande identitetsuppgifter behandlas för användaradministration
- Känsliga personuppgifter och sekretess är förbjudna
- Endast kontext (ej användaridentifierande info) delas med AI-leverantörer

3. Privacy by design:

- Svenska/EU-baserade modeller rekommenderas som förstahandsval
- Användare gör informerade val vid användning av amerikanska modeller
- Alternativa arbetssätt finns tillgängliga

4. Tydlig ansvarsfördelning:

- Personuppgiftsbiträdesavtal med Intric AB
- Dokumenterade DPA:er med AI-leverantörer (OpenAI, Anthropic)
- Underbiträdesavtal med infrastrukturleverantörer (Glesys, Airon)

5. Certifieringar och standarder:

- Intric AB: ISO 27001:2022 (certifikat ACCISMS2025110188), INFORMATIONSSÄKERHETSKRAV 3-3-3
- AI-leverantörer: SOC 2 Type II (OpenAI), SOC 2 (Anthropic)
- Datacenter: Glesys AB med hög säkerhetsstandard i Sverige

Slutsats

Förhandssamråd bedöms inte som nödvändigt. Kommunen kan genomföra behandlingen under förutsättning att fastställda åtgärder och rutiner följs.

Resultatet av eventuellt förhandssamråd

Inget förhandssamråd har genomförts då skyldigheten inte föreligger.

Steg 7. Synpunkter som hämtats in från berörda

7.1 Dataskyddsombudets rekommendationer

Underskrift: [Dataskyddsombudets signatur]

(För den tidigare versionen har dataskyddsombudet Frida Sjökvist lämnat sitt yttrande avseende konsekvensbedömningen. Yttrandet har resulterat i följande rekommendationer och åtgärder:

– Val av rättslig grund: DSO rekommenderar artikel 6.1 e (uppgift av allmänt intresse). Åtgärd: Reviderad, se avsnitt 4.2.

– Ändamålsglidning och felaktig information: DSO identifierar ytterligare risker. Åtgärd: R12 och R13 tillagda, se Steg 5.

– Transfer Impact Assessment: DSO rekommenderar formell TIA. Åtgärd: Genomförd, se avsnitt 4.4

– Registrerades rättigheter: DSO påpekar praktiska begränsningar. Åtgärd: Förtydligat i avsnitt 4.3.

– AI-förordningen: DSO rekommenderar beaktande. Åtgärd: Integrerad i avsnitt 4.1 och 10.1.)

7.2 Synpunkter från de registrerade

Medarbetare

Synpunkter från medarbetare (kommunens anställda) har hämtats in genom:

1. Pilotgrupp:

Innan full utrullning av Intric-plattformen genomfördes en pilottest med en mindre grupp medarbetare (ca 20 personer) från olika verksamhetsområden. Pilotgruppen fick:

- Utbildning om Intric-plattformen och dataskyddsaspekter
- Möjlighet att testa plattformen under sex månader
- Uppföljning för att dela synpunkter

Synpunkter från pilotgruppen:

Positivt:

- Majoriteten upplevde plattformen som användbar och tidsbesparande för textproduktion och administrativa uppgifter
- Användargränssnittet upplevdes som intuitivt
- Möjligheten att välja mellan olika modeller uppskattades

Oro för dataskydd:

- Några uttryckte oro för hur personuppgifter hanteras, särskilt vid användning av amerikanska AI-modeller
- Frågor kring vad som händer med konversationshistoriken

Behov av tydligare riktlinjer:

- Vissa upplevde osäkerhet kring vad som är tillåtet att behandla i plattformen
- Önskemål om fler praktiska exempel i utbildningsmaterialet

Åtgärder baserat på synpunkter:

- Riktlinjerna för AI har tagits fram.
- Utbildningsmaterialet har tagits fram
- Information om var data lagras har förtydligats för varje modell
- Privacy by design-rekommendation har lagts till (svenska/EU-modeller som förstahandsval)
- Tydlig information om lagringstider och radering har lagts till

2. Fackliga representanter:

Externa personer

Eftersom externa personer vars personuppgifter kan förekomma i användarinteraktioner (t.ex. namn i en projektplan) inte har direkt kontakt med Intric-plattformen, har inga specifika synpunkter hämtats in från dessa i förväg.

Motivering:

Att hämta in synpunkter från potentiellt alla externa personer vars namn eller kontaktuppgifter kan komma att förekomma i kommunens användning av AI-verktyget bedöms som **oproportionerligt och ogenomförbart** eftersom:

- Det är okänt i förväg vilka personer som kan komma att beröras
- De personuppgifter som behandlas är begränsade till grundläggande kontaktuppgifter (namn, e-post, telefonnummer)
- Känsliga personuppgifter och sekretess är förbjudna
- Lagringstiden är begränsad (max 30 dagar hos AI-leverantörer, 3 månader i Intric)

- Externa personer kan rimligen förvänta sig att kommunen använder digitala verktyg för att hantera information i samband med samarbeten och kommunikation

Åtgärder för att tillgodose externa personers intressen:

- Allmän information på kommunens webbplats om användning av AI-verktyg i integritetspolicyn
- Tydliga kontaktuppgifter för frågor och utövande av rättigheter (dataskyddsombud, systemförvaltare)
- Möjlighet för externa personer att invända mot behandling om de har berättigade skäl
- Information kan lämnas vid specifika tillfällen när det är lämpligt (t.ex. i projektsammanhang)

7.3 Synpunkter från övriga intressenter

Systemförvaltaren

Systemförvaltaren har varit involverad i planeringen och har lämnat synpunkter på tekniska aspekter:

Synpunkter:

- Krav på säkerhetskopiering: Betonade vikten av att säkerhetskopior finns och att återställning kan ske vid incident
- Integration med AD: Önskemål om integration med Active Directory för automatisk provisionering av användarkonton
- Loggning: Behov av centraliserad loggning för att underlätta säkerhetsövervakning

Åtgärder baserat på synpunkter:

- Säkerhetskopiering ingår som del av tjänsten hos Glesys (dagliga inkrementella, veckovisa fulla backuper)
- Integration med AD utreds för framtida implementation
- Loggdata från Intric kan integreras med kommunens SIEM-system

Informationssäkerhetsansvarig

Informationssäkerhetsansvarig har granskat säkerhetsaspekterna och lämnat följande synpunkter:

Synpunkter:

- Certifieringar: Positivt att Intric och Glesys har ISO 27001-certifiering
- Kryptering: Bekräftelse att all kommunikation sker krypterat (SSL/TLS)
- Incidenthantering: Behov av tydliga rutiner för hantering av personuppgiftsincidenter
- Regelbunden översyn: Rekommendation att säkerhetsöversyn genomförs årligen

- INFORMATIONSSÄKERHETSKRAV-bedömning: Rekommendation att verifiera INFORMATIONSSÄKERHETSKRAV-nivå

Åtgärder baserat på synpunkter:

- Certifieringar verifierade: ISO 27001:2022 (certifikat ACCISMS2025110188), INFORMATIONSSÄKERHETSKRAV 3-3-3
- Kryptering bekräftad: SSL/TLS för kommunikation, AES-256 för data i vila
- Årlig säkerhetsöversyn har inkluderats i uppföljningsplanen
- INFORMATIONSSÄKERHETSKRAV 3-3-3 verifierad med fullständig genomgång av alla 93 krav

Sammanfattning – Synpunkter från berörda:

Dataskyddsombudets rekommendationer har beaktats och åtgärder har vidtagits. Synpunkter från medarbetare (via pilotgrupp och fackliga representanter) har lett till förbättringar av riktlinjer, utbildning, privacy by design-implementering och val av standardmodell. Tekniska och säkerhetsmässiga synpunkter från Systemförvaltaren och informationssäkerhetsansvarig har integrerats i lösningen. För externa personer bedöms det som oproportionerligt att hämta in synpunkter i förväg, men information och kontaktvägar finns tillgängliga.

Steg 8. Sammantagen bedömning

Efter genomförd konsekvensbedömning, inklusive systematisk beskrivning av behandlingen, rättslig analys, riskhantering och inhämtande av synpunkter från berörda, görs bedömningen att den planerade personuppgiftsbehandlingen **kan genomföras**.

Grunder för bedömningen

1. Tydlig rättslig grund och efterlevnad av dataskyddsprinciper

Behandlingen har tydlig och giltig rättslig grund:

- **Uppgift av allmänt intresse (artikel 6.1 e GDPR)** för medarbetares användaruppgifter

Samtliga grundläggande dataskyddsprinciper följs genom omfattande tekniska och organisatoriska åtgärder:

- Laglighet, korrekthet och öppenhet
- Ändamålsbegränsning
- Uppgiftsminimering
- Riktighet
- Lagringsminimering
- Integritet och konfidentialitet

2. Nödvändighet och proportionalitet

Behandlingen är **nödvändig** för att möjliggöra för kommunens medarbetare att använda moderna AI-verktyg för att effektivisera sitt arbete och höja kvaliteten i kommunikation och service till invånare. De specificerade ändamålen är noga avgränsade till områden där känsliga personuppgifter och sekretess inte förekommer.

Behandlingen är **proportionerlig** eftersom:

- Endast grundläggande identitetsuppgifter om medarbetare behandlas för plattformsadministration (namn, e-post, användar-ID)
- Personuppgifter om externa personer som kan förekomma i användarinteraktioner är begränsade till grundläggande kontaktuppgifter (namn, e-post, telefonnummer)
- Tydliga riktlinjer och tekniska varningar förhindrar att känsliga uppgifter eller sekretess hanteras
- **Privacy by design** implementeras genom rekommendation av svenska/EU-baserade modeller som förstahandsval
- Omfattande säkerhetsåtgärder minimerar riskerna:
- ISO 27001:2022-certifiering (certifikat ACCISMS2025110188)
- INFORMATIONSSÄKERHETSKRAV 3-3-3 uppfyllt med verifierade säkerhetsåtgärder
- SOC 2 certifieringar hos AI-leverantörer
- Alternativa metoder (manuell textproduktion, externa konsulter) skulle vara betydligt mer kostsamma och tidskrävande

3. Effektiv riskhantering

Riskhanteringen har identifierat potentiella risker för enskildas fri- och rättigheter och för varje risk har riskreducerande åtgärder identifierats och implementerats. Efter beaktande av åtgärderna bedöms de kvarvarande riskerna som **acceptabla**. Ingen hög risk kvarstår.

Särskilda åtgärder för högsta riskerna:

- **R01 (Känsliga uppgifter):** Omfattande utbildning, tydliga UX-varningar, incidenthantering
- **R04 (OpenAI/Anthropic):** Dokumenterade DPA:er med SCC, max 30 dagars lagring, privacy by design-rekommendation, användare gör informerat val

4. Registrerades rättigheter kan tillgodoses

Rutiner och processer finns för att säkerställa att registrerades rättigheter enligt GDPR kan tillgodoses:

- Rätt till information (via utbildning, intranät, integritetspolicy)

- Rätt till tillgång (via Systemförvaltare)
- Rätt till rättelse (via Systemförvaltare)
- Rätt till radering (automatisk gallring + radering på begäran)
- Rätt till begränsning av behandling
- Rätt att göra invändningar
- Skydd mot automatiserat beslutsfattande (AI används endast som stödverktyg)

Informationsansvar uppfylls genom proaktiv information och tydliga kontaktvägar.

5. Beaktande av synpunkter

Synpunkter från dataskyddsombud, medarbetare (pilotgrupp, fackliga representanter), Systemförvaltaren och informationssäkerhetsansvarig har beaktats och lett till förbättringar:

- Privacy by design-rekommendation av svenska/EU-modeller
- Förtydligade riktlinjer och utökad utbildning
- Dokumenterade DPA:er med AI-leverantörer
- INFORMATIONSSÄKERHETSKRAV 3-3-3 verifiering
- Tydlig information om loggning och lagringstider

6. Certifieringar och avtal

Intric AB och underleverantörer har relevanta certifieringar och dokumenterade avtal:

- **Intric AB:** ISO 27001:2022, INFORMATIONSSÄKERHETSKRAV 3-3-3
- **Glesys AB:** Datacenter i Sverige med hög säkerhetsstandard
- **OpenAI:** DPA med SCC Module Two (24 jan 2024), SOC 2 Type II, max 30 dagars lagring
- **Anthropic:** DPA med SCC Module Two och Three (24 feb 2025), SOC 2, max 30 dagars lagring
- Personuppgiftsbiträdesavtal och underbiträdesavtal reglerar ansvarsfördelning och säkerhetsåtgärder

7. Uppföljning och kontinuerlig förbättring

Planer finns för regelbunden uppföljning av behandlingen för att säkerställa att:

- Riktlinjer följs
- Risker hanteras
- Förändringar i riskbild eller rättsläge uppmärksammas i tid

- Privacy by design-principen upprätthålls i praktiken

Slutsats

Sammantaget bedöms behandlingen vara **nödvändig, proportionerlig och förenlig** med dataskyddsförordningen och kompletterande lagstiftning. Den kan därmed genomföras under förutsättning att fastställda rutiner, riktlinjer, säkerhetsåtgärder och uppföljning upprätthålls kontinuerligt.

Villkor för genomförande

Behandlingen får endast genomföras om följande villkor uppfylls:

1. **Kommunens riktlinjer för användning av Intric** ska följas av alla användare
2. **Tekniska varningar i användargränssnittet** ska finnas kvar och visas konsekvent
3. **Privacy by design:** Svenska/EU-baserade modeller (Managed by Intric, Llama 3.3 SWE, Mistral) rekommenderas som förstahandsval för arbetsuppgifter som kan innehålla personuppgifter
4. **Utbildning** ska ges till alla medarbetare som får tillgång till plattformen (Basutbildning i AI, instruktionsfilmer, utbildningsmaterial)
5. **Systemförvaltaren** ska genomföra regelbunden uppföljning av användning och säkerhet
6. **Dataskyddsombud** ska involveras vid uppföljning och vid eventuella förändringar
7. **Konsekvensbedömningen** ska uppdateras vid väsentliga förändringar i behandlingen, riskbilden eller rättsläget
8. **Dokumenterade DPA:er** med AI-leverantörer ska upprätthållas och ses över vid förändringar
9. **Rättsläget** ska bevakas kontinuerligt, särskilt avseende tredjelandsöverföringar och SCC:s giltighet

Steg 9. Förankring av bedömningen i organisationen

Konsekvensbedömningen har förankrats i Lidköpings kommuns organisation enligt följande:

Presentation för ledningsgruppen

Konsekvensbedömningen presenterades för **[relevant ledningsgrupp/nämnd]** vid möte den **[datum]**. Presentationen inkluderade:

- Översikt av Intric-plattformen och dess funktioner
- Beskrivning av personuppgiftsbehandlingen

- Identifierade risker och riskreducerande åtgärder
- Rättslig analys och slutsatser
- Privacy by design-principen och rekommendation av svenska/EU-modeller
- Villkor för genomförande
- Plan för kontinuerlig uppföljning

Beslut: Ledningsgruppen godkände konsekvensbedömningen och beslutade att behandlingen kan genomföras enligt de villkor som anges.

Förankring med dataskyddsombud

Dataskyddsombudet har varit involverat löpande under hela processen och har lämnat sitt slutliga utlåtande **[datum]**, där det rekommenderar att behandlingen kan genomföras under förutsättning att fastställda villkor följs.

Samråd med Systemförvaltaren och informationssäkerhetsansvarig

Systemförvaltaren och informationssäkerhetsansvarig har granskat tekniska och säkerhetsmässiga aspekter och bekräftat att föreslagna åtgärder är adekvata och genomförbara.

Information till berörda medarbetare

Information om konsekvensbedömningens slutsatser och villkor för användning av Intric-plattformen har kommunicerats till alla medarbetare som ska ges åtkomst via:

- E-post med sammanfattning och länkar till fullständig information
- Publicering på intranätet
- Utbildningstillfällen (Basutbildning i AI, instruktionsfilmer)

Dokumentation av ansvarsfördelning

Följande ansvarsfördelning har fastställts enligt förvaltningsplanen och kommunens organisatoriska struktur:

Ansvar	Roll/Funktion
Yttersta ansvar för att behandlingen följer GDPR	Respektive nämnd
Systemägare – Beslutsfattare för drift, utveckling och budget	Chef Verksamhetsutveckling och Digitalisering

Ansvar	Roll/Funktion
Systemförvaltare – Ansvarar för daglig drift, support och förändringshantering	Systemförvaltare VoD
Systemadministratör (per sektor) – Hanterar behörigheter och driftstöd inom egen sektor, ger tekniskt stöd till användare	Utvecklingsledare/systemförvaltare eller motsvarande från respektive sektor/bolag
Förvaltningsgrupp – Hanterar löpande frågor gällande drift och utveckling	Systemförvaltare, systemadministratör, systemägare, vid behov repr. från VoD.
Funktionsansvarig (per assistent/assistentgrupp) – Ansvarig för att respektive framtagen assistent fungerar som den ska, stödjer användare	Respektive systemadministratör utser funktionsansvarig per assistent
IT-driftsansvarig – Säkerställer teknisk drift och säkerhet relaterat till lokal infrastruktur	Leverantör/Systemförvaltare
Informationssäkerhetsansvarig (CISO) – Följer upp informationssäkerhet, stödjer chefer med information och utbildning	Informationssäkerhetsstrateg
Ansvar för genomförande av riskreducerande åtgärder (tekniska)	Leverantör
Ansvar för genomförande av riskreducerande åtgärder (organisatoriska - riktlinjer, utbildning)	Systemförvaltare och Systemadministratörer
Ansvar för uppföljning av användning och efterlevnad av riktlinjer	Förvaltningsgrupp i samråd med dataskyddsombud/CISO
Ansvar för uppföljning av privacy by design-principen	Systemförvaltare i samråd med dataskyddsombud/CISO
Ansvar för bevakning av rättsläget (tredjelandsöverföringar, SCC)	Dataskyddsombud i samarbete med jurist
Ansvar för hantering av kvarvarande risker	Respektive nämnd
Ansvar för uppdatering av konsekvensbedömningen vid behov	Systemförvaltare i samråd med dataskyddsombud

Kvarvarande risker

De kvarvarande riskerna (som bedömts som acceptabla efter riskreducerande åtgärder) ägs av respektive nämnd som personuppgiftsansvarig. Dessa risker följs upp kontinuerligt enligt fastställd plan.

Identifierade kvarvarande risker:

- **R01:** Risk för att känsliga uppgifter inkluderas trots förbud (kräver kontinuerlig utbildning)
- **R04:** Risk vid användning av amerikanska AI-modeller (kräver bevakning av rättsläge)
- **R09:** Risk för förändringar i rättsläge (kräver kontinuerlig bevakning)

Beslut om genomförande

Beslut om att genomföra behandlingen och införa Intric-plattformen fattades av **[beslutsfattare]** den **[datum]** med referens till denna konsekvensbedömning.

Sammanfattning – Förankring:

Konsekvensbedömningen har presenterats och godkänts av ledningen. Ansvarsfördelning för genomförande av åtgärder och hantering av kvarvarande risker är tydligt dokumenterad. Berörda medarbetare har informerats om villkoren för användning. Detta säkerställer att konsekvensbedömningen är känd och accepterad på relevanta nivåer i organisationen och att nödvändiga åtgärder kan vidtas kontinuerligt.

Steg 10. Kontinuerlig översyn

10.1 Plan för att genomföra översyn

Konsekvensbedömningen för Intric-plattformen ska följas upp kontinuerligt för att säkerställa att behandlingen fortsätter att följa dataskyddsförordningen och att riskerna förblir under kontroll.

Regelbunden översyn

Konsekvensbedömningen ska ses över enligt följande schema:

1. Löpande övervakning

- **Ansvarig:** Systemförvaltaren
- **Frekvens:** Kontinuerligt
- **Åtgärder:**
- Övervakning av säkerhetsloggar via SIEM för att upptäcka avvikelser
- Hantering av användarfeedback och rapporterade problem
- Uppföljning av incidenter och avvikelser
- Verifiering att tekniska varningar i UX fungerar

2. Kvartalsvis uppföljning

- **Ansvarig:** Systemförvaltare i samråd med dataskyddsombud och förvaltningsgrupp
- **Frekvens:** Varje kvartal (enligt förvaltningsplanens möte "Avstämning rutiner")
- **Åtgärder:**
- Granskning av användarstatistik och identifiering av avvikande användningsmönster
- Kontroll av att automatisk gallring fungerar korrekt
- Översyn av eventuella incidenter eller klagomål från registrerade
- Verifiering av att riktlinjer och informationstexter är aktuella
- Uppföljning av rutiner och förändringsbehov enligt förvaltningsplanen
- **Uppföljning av privacy by design:** Kontroll av hur ofta svenska/EU-modeller används jämfört med amerikanska modeller

3. Årlig översyn

- **Ansvarig:** Systemförvaltare, dataskyddsombud, informationssäkerhetsansvarig, IT-driftsansvarig
- **Frekvens:** Minst en gång per år (enligt förvaltningsplanens årliga planeringsmöte i februari och avstämning teknik juni/december)
- **Åtgärder:**
- Fullständig genomgång av konsekvensbedömningen
- Översyn av risker och riskreducerande åtgärder – har nya risker uppstått?
- Kontroll av att lagringstider fortfarande är motiverade
- Verifiering av att personuppgiftsbiträdesavtal och underbiträdesavtal är aktuella
- **Kontroll av leverantörers certifieringar:**
- ISO 27001:2022 (Intric AB)
- INFORMATIONSSÄKERHETSKRAV 3-3-3 (Intric AB)
- SOC 2 (OpenAI, Anthropic)
- **Bevakning av DPF-status:** Kontroll om OpenAI eller Anthropic har blivit certifierade enligt EU-U.S. Data Privacy Framework
- **Kontroll av SCC:s giltighet:** Bevakning av om EU-kommissionen har uppdaterat eller återkallat SCC
- Utvärdering av om alternativa lösningar eller leverantörer bör övervägas
- Driftstatus och kommande ändringar från leverantör
- **Utvärdering av privacy by design:** Analys av användningsstatistik för olika modeller

- Uppdatering av konsekvensbedömningen vid behov

Översyn vid väsentliga förändringar

Konsekvensbedömningen ska uppdateras **omgående** vid följande händelser:

1. Nya AI-modeller eller leverantörer läggs till

- Riskbedömning ska göras för nya leverantörer
- Verifiering av DPA:er och SCC
- Bedömning av geografisk placering

2. Nya användningsområden eller ändamål

- Om Intric börjar användas för andra ändamål än de specificerade

3. Förändringar i rättsläge:

- **Upphävande eller förändring av EU-U.S. Data Privacy Framework**
- **Nya riktlinjer från IMY eller EDPB** som påverkar användningen av AI-verktyg eller tredjelandsöverföringar
- **Nya domar från EU-domstolen** som påverkar behandlingen (t.ex. ny "Schrems"-dom)
- **Förändringar i amerikansk lagstiftning** som påverkar CLOUD Act eller FISA 702

4. Säkerhetsincidenter

- Om en personuppgiftsincident inträffar ska riskbedömningen ses över
- Bedömning av om åtgärderna var tillräckliga

5. Organisatoriska förändringar

- Om ansvarsfördelningen förändras
- Om nya verksamhetsområden får tillgång
- Om förvaltningsmodellen ändras

6. Tekniska förändringar

- Om Intric-plattformen får nya funktioner
- Om dataflödet förändras
- Om nya integrationer införs

7. Förändringar i leverantörskedjan

- Om Intric byter underleverantör (t.ex. Glesys, Airon)
- Om AI-modelleverantörer ändrar sina villkor eller DPA:er väsentligt

Ansvarig för att identifiera och initiera översyn vid förändringar

Ansvarsområde	Ansvarig roll
Bevaka tekniska och leverantörsrelaterade förändringar	Systemförvaltare
Bevaka teknisk säkerhet relaterat till lokal infrastruktur	IT-driftsansvarig
Bevaka förändringar i rättsläge och regulatorisk vägledning	Dataskyddsombud i samarbete med jurist
Livscykelhantering av assistenter och säkerställa att de är aktuella	Funktionsansvariga
Meddela systemförvaltare om nya användningsområden planeras	Verksamhetsansvariga

Rutiner för att fånga upp förändringar

1. Prenumeration på nyheter:

- Systemförvaltaren och dataskyddsombud prenumererar på nyheter från IMY, EDPB och relevanta branschtidskrifter
- Bevakning av Privacy Shield Framework-listan för eventuell DPF-certifiering av OpenAI/Anthropic

2. Leverantörskommunikation:

- Regelbunden dialog med Intric AB om planerade förändringar i tjänsten
- Prenumeration på Intricssubprocessor-lista för att få notifieringar om nya underbiträden

3. Incidentrapportering:

- Rutiner för att rapportera och utreda säkerhetsincidenter finns dokumenterade i kommunens informationssäkerhetspolicy
- Incident Response Plan hos Intric AB med anmälningsplikt till kommunen

4. Användarfeedback:

- Kanaler för medarbetare att rapportera problem eller frågor
- Regelbundna användarenkäter

5. Samverkan med andra kommuner:

- Deltagande i nätverk för erfarenhetsutbyte kring AI-verktyg
- Delning av erfarenheter kring tredjelandsöverföringar och rättsläge

Dokumentation av översyn

Varje översyn ska dokumenteras med:

- **Datum för översynen**
- **Deltagare**
- **Identifierade förändringar eller avvikelser**
- **Åtgärder som vidtagits**
- **Beslut om konsekvensbedömningen behöver uppdateras eller inte**
- **Uppföljning av privacy by design-principen** (användningsstatistik för svenska/EU-modeller vs amerikanska modeller)

Dokumentationen förvaras tillsammans med konsekvensbedömningen.

Sammanfattning – Kontinuerlig översyn:

En strukturerad plan för kontinuerlig översyn säkerställer att konsekvensbedömningen hålls aktuell och att förändringar i riskbild, rättsläge eller behandling fångas upp i tid. Särskild vikt läggs vid:

- **Privacy by design:** Uppföljning av att svenska/EU-modeller används enligt rekommendation
- **Tredjelandsöverföringar:** Kontinuerlig bevakning av DPF-status och SCC:s giltighet
- **Rättsläge:** Bevakning av EU-domstolens praxis och nya riktlinjer från IMY/EDPB

Tydlig ansvarsfördelning och dokumenterade rutiner garanterar att uppföljningen genomförs systematiskt. Versionshistorik ger spårbarhet och möjlighet att följa behandlingens utveckling över tid.

Slutsats

Denna konsekvensbedömning för användningen av Intric AI-plattform i Lidköpings kommun visar att behandlingen **kan genomföras i enlighet med dataskyddsförordningen** under förutsättning att fastställda riktlinjer, säkerhetsåtgärder och uppföljningsrutiner följs.

Sammanfattning av slutsatser

1. Rättslig grund och dataskyddsprinciper:

- har tydlig rättslig grund: artikel 6.1 e GDPR (uppgift av allmänt intresse) med stöd i kommunallagen (2017:725)
- Samtliga dataskyddsprinciper följs
- Privacy by design implementeras genom rekommendation av svenska/EU-modeller

2. Risker:

- Omfattande tekniska och organisatoriska åtgärder minimerar riskerna för enskildas fri- och rättigheter
- Certifieringar (ISO 27001:2022, INFORMATIONSSÄKERHETSKRAV 3-3-3, SOC 2) bekräftar säkerhetsnivån
- Kvarvarande risker bedöms som acceptabla med kontinuerlig uppföljning

3. Tredjelandsöverföringar:

- Dokumenterade DPA:er med SCC skyddar överföringar till USA
- Endast kontext (ej användaridentifierande info) delas med amerikanska leverantörer
- Max 30 dagars lagring hos AI-leverantörer
- Privacy by design-rekommendation ger användare kontroll

4. Registrerades rättigheter:

- Rutiner finns för att tillgodose alla rättigheter enligt GDPR
- Proaktiv information till medarbetare och externa personer
- Tydliga kontaktvägar för frågor och utövande av rättigheter

5. Uppföljning:

- Strukturerad plan för kontinuerlig översyn (kvartalsvis, årlig)
- Tydlig ansvarsfördelning
- Rutiner för att fånga upp förändringar i riskbild och rättsläge

Villkor för fortsatt behandling

Behandlingen får endast fortsätta om:

1. Kommunens riktlinjer följs konsekvent
2. Privacy by design-principen upprätthålls i praktiken
3. Utbildning ges till alla nya användare
4. Kontinuerlig uppföljning sker enligt plan
5. Dataskyddsombud involveras vid förändringar
6. Rättsläget bevakas särskilt avseende tredjelandsöverföringar
7. Konsekvensbedömningen uppdateras vid väsentliga förändringar

Bilagor

Bilaga 1: Riskhantering vid konsekvensbedömning (Excelblad)

Bilaga 2: Data Processing Addendum - Intric AB och OpenAI (24 januari 2024)

Bilaga 3: Data Processing Addendum - Intric AB och Anthropic (24 februari 2025)

Bilaga 4: Personuppgiftsbiträdesavtal - Lidköpings kommun och Intric AB

Bilaga 5: Riktlinjer för artificiell intelligens (AI) – Lidköpings kommunkoncern

Bilaga 6: Förvaltningsplan Intric AI 2025-2026

Bilaga 7: Informationssäkerhetspolicy – Lidköpings kommun (2024)

Bilaga 8: INFORMATIONSSÄKERHETSKRAV 3-3-3 bedömning - Intric AB

Bilaga 9: ISO 27001:2022 certifikat - Intric AB (ACCISMS2025110188)

(Då flera av ovanstående bilagor är NDA behöver de delas ut på ett säkert sätt)