Molntjänster i verksamheten

SOURCINGBESLUT OCH SAMMANFATTNING AV RÄTTSLIGA FRÅGOR - EN VÄGLEDNING FÖR KOMMUNER OCH REGIONER I ARBETET MED ATT UTVECKLA VERKSAMHETEN I EN DIGITAL TID, V 1.1 20191111

Sveriges Kommuner och Landsting

Innehållsförteckning

Inledning och syfte med dokumentet 3

Sammanfattning 3

Sourcing och molntjänster 4

Digitalisering och välfärdsutmaningen 4

Användning av molntjänster 4

Molntjänster och säkerhet 5

Strategi och hantering av nuläget 6

Sammanfattning av rättsliga frågor 7

Statlig utredning 7

Dataskydd 8

Detta gör SKL 8

Inledning och syfte med dokumentet

Målgrupp för denna PM är rollerna it-chef, CIO, digitaliseringschef och ledning i kommuner och regioner. Dokumentet är tänkt att erbjuda en möjlighet att orientera sig om användningen av moln för hantering av verksamhets-information och det rättsliga nuläget som kan ha en påverkan på beslut om utkontraktering eller sourcing.

Nedan ges en översikt av områden och perspektiv som aktualiseras i samband med användning av molntjänster. Dokumentet utgör en översikt och summering av information i SKLs vägledningar:

- **Molntjänster och konfidentialitetsbedömning**
  Denna vägledning beskriver ett metodstöd för analys och ger även en översökt över olika typer av molntjänster

- **Fakta-PM om CLOUD Act**

Sammanfattning

Kommuner och regioner samt även statliga myndigheter har under lång tid haft som mål att digitalisera, genom de olika satsningar, investeringar och mål som styr offentlig sektor[1]. Digitaliseringsstrategin anger inriktningen för regeringens digitaliseringspolitik och det övergripande målet är att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter, kunna driva innovation där målmedveten ledning och infrastruktur är viktiga förutsättningar.

Digitaliseringen inom kommuner och regioner har två grundläggande syften, att effektivisera tjänsteleveransen till invånaren både ur ett kostnadsperspektiv och ur perspektivet att förenkla invånarens dialog med parterna i offentlig sektor. Båda dessa syften kräver goda förutsättningar för innovation kopplat till informationshantering, dvs att vi radikalt ändrar hur vi bearbetar och lagrar information. För att uppnå digital mognad och dra nytta av teknikutvecklingen behöver vi lämna arvet av tidigare digitala initiativ bakom oss. För många innebär det att flytta arbetssätten till publika eller privata molntjänster då det ger en större möjlighet att genomföra transformationen och samtidigt följa principen om det mest kostnadseffektiva alternativet.

När nu grundläggande rättsliga förutsättningar för denna övergång ifrågasätts under pågående transformation uppstår en osäkerhet som medför en uppbromsning.

[1] Se nu gällande Digitaliseringsstrategin, Infrastrukturdepartementet, https://www.regeringen.se/regeringens-politik/digitaliseringsstrategin/

SKLs styrelse har identifierat att uppbromsningen skapar en konflikt med antagna mål och har beslutat om ett ställningstagande gällande molntjänster:

Läs SKLs ställningstagande här.

Sourcing och molntjänster

Digitalisering och välfärdsutmaningen

Frågeställningen om användandet av molntjänster och sourcing samt de rättsliga utmaningarna måste ses i ljuset av de välfärdsutmaningar som kommuner och regioner står inför. Läs mer om välfärdsutmaningarna i SKLs ekonomirapport från oktober 2019.

Trots uppenbar rättslig osäkerhet just nu när det gäller förutsättningar för användning av molntjänster, finns fortfarande ett stort behov av användning och alternativet att ”backa” eller ”ta hem” till egen drift är ofta inte möjligt att genomföra. Redan genomförda omställningar för att skapa förmåga att digitalisera verksamheten och gjorda investeringar för att möta de nationella målen om digitalisering[2] medför att det saknas förmåga att hantera drift i egen regi, som det gjordes förr.

En återgång till mer traditionell it-drift medför konsekvenser i form av kostnader som måste vara mycket väl motiverade för att kunna vara i linje med god ekonomisk hushållning. I en undersökning från Radar[3] beskrivs ekonomiska utmaningar för kommunernas it-budget över tid och kopplat till investeringar, utveckling och molntjänster.

Rapporten berör även prioriteringar som påverkas av det osäkra rättsläget[4]:

”Den senaste tiden har präglats av en stor försiktighet inom offentlig sektor vad gäller investeringar i it. På sikt kommer försiktigheten, som till stor del härrör ur osäkerhet kring molntjänster, behöva ersättas av en strävan att fortsätta driva verksamhetsförändringar för att inte halka efter i användandet av ny teknik samt dra nytta av effekterna av standardiserad och industrialiserad it.”

Användning av molntjänster

Kommuner och regioner använder i stor utsträckning olika typer av moln-tjänster. Nyttjandet varierar från användning av dedikerade lösningar för viss del av verksamheten till beroende genom strategiska vägval för infrastruktur och centrala administrativa stödresurser.

[2] Digitaliseringsstrategin, Regeringen, Infrastrukturdepartementet. https://www.regeringen.se/regeringens-politik/digitaliseringsstrategin/
[3] Radar Ecosystem Specialists; Moln över kommunerna – hot eller möjlighet, Rapport 2019 (nedan: Radar rapporten).
[4] Radar rapporten, sid 10.

En utmaning för kommuner och regioner är att användningen sällan handlar om ren lagring, dvs information i vila. I de flesta fall handlar det om hela processen att skapa, hämta in, bearbeta, analysera, dela/publicera och lagra/arkivera samt gallra information. Tjänstebehovet omfattar alltså hela informationens livscykel samt alla stadier som vila, bearbetning och förflyttning. Detta ställer stora krav på skyddsfunktioner och avtalad möjlighet till insyn och granskning av hanteringen.

Undersökningen från Radar visar att cirkaa 50 procent av kommunerna använder Microsoft Office 365 (MS O365) och att 100 procent av de större kommunerna använder denna tjänst.

Molntjänster och säkerhet

Molntjänster kan med rätt kravställning och införande ge en betydligt högre nivå av it-säkerhet än vad it-drift i egen regi kan åstadkomma. Det finns flera skäl till detta, bland annat förmåga att hålla säkerhetsuppdateringar, utrusta med rätt skydd i form av ny programvara, bevakning av teknikutveckling, personal som har kompetens att hantera nya typer av hot och risker och förmågan att övervaka och följa upp. Mot detta behöver ställas risker för informationshanteringen som uppstår av globala molntjänsteleverantörer med flera länders rättssystem att ta hänsyn till, komplexa affärsmodeller och omfattande avtalskonstruktioner.

All informationshantering innebär risk och den vedertagna metoden för att minska risker är att arbeta med flera olika typer av analyser för att identifiera vilka säkerhetshöjande och riskreducerande åtgärder som behöver vidtas. Ur detta perspektiv skiljer sig inte molntjänster från det arbete med kravställning och uppföljning som behöver göras i förhållande till andra typer av tjänster och leverantörer samt hantering av egen anställd personal.

När det gäller användning av publika molntjänster med standardiserade avtalsvillkor blir det däremot en annan process eftersom man istället måste granska tjänsten, vilka säkerhetsmekanismer som finns och analysera ifall tjänstens utformning och villkor lämpar sig för de behov verksamheten har och de krav på säkerhet som informationen kräver.

Vägledning och etablerade analysmetoder för till exempel riskanalys finns i Metodstöd för systematiskt informationssäkerhetsarbete, som tillhandahålls av MSB med flera myndigheter på www.informationssakerhet.se.

En av nyckelanalyserna är att genomföra informationsklassning av den information som ska hanteras i en molntjänst. Med hjälp av en sådan klassning av olika informationsmängder får verksamheten en nödvändig grund för att kunna formulera krav gentemot leverantör och tjänst. Inför användning av molntjänster är det avgörande att veta vilken information i verksamheten som behöver vilken nivå av skydd, eftersom den tilltänkta molntjänsten måste matchas till informationen.

SKL tillhandahåller verktyget KLASSA för att underlätta informationsklassning.

Även om rättsläget för närvarande är osäkert är informationsklassning och riskanalyser ett arbete som är nödvändigt att genomföra, oavsett om informationshanteringen kommer att ske med egen it-drift, hos traditionell systemleverantör eller i molntjänst.

I SKLs vägledning ”Molntjänster och konfidentialitetsbedömning” finns ett metodstöd och en processbild som stöd för analysarbetet.

Strategi och hantering av nuläget

Det råder just nu viss rättslig osäkerhet inom flera områden som är viktiga att bedöma inför användning av molntjänster. Därför föreslår SKL försiktighet och noga överväganden i samband med nya upphandlingar som kan involvera molntjänster. Molntjänster ska generellt inte undvikas - tvärtom – de kan ofta vara den mest effektiva lösningen. Däremot bör verksamheten säkerställa att analys av säkerhet och rättsliga frågor genomförs för att identifiera vilket behov av skydd som behövs för olika typer av information så att konfidentiell eller känslig information inte hanteras fel. Som vi tidigare påpekat i detta dokument är detta något som alltid ska göras vid all hantering av information oavsett vilka vägval som analysen resulterar i. Detta är inte en följd av det osäkra rättsläget, utan en följd av att allt mer information hanteras digitalt och både den rättsliga och informationssäkerheten alltid ska vara en del av riskbedömningen.

Till stor del blir det fråga om att skapa en process för att säkerställa att dessa analyser genomförs inför användning av molntjänster, så att beslut riskavvägning även kan dokumenteras.

Det finns även behov av att ur ett strategiskt perspektiv överväga ytterligare faktorer med användning av publika molntjänster med standardiserade avtalsvillkor, som till exempel:

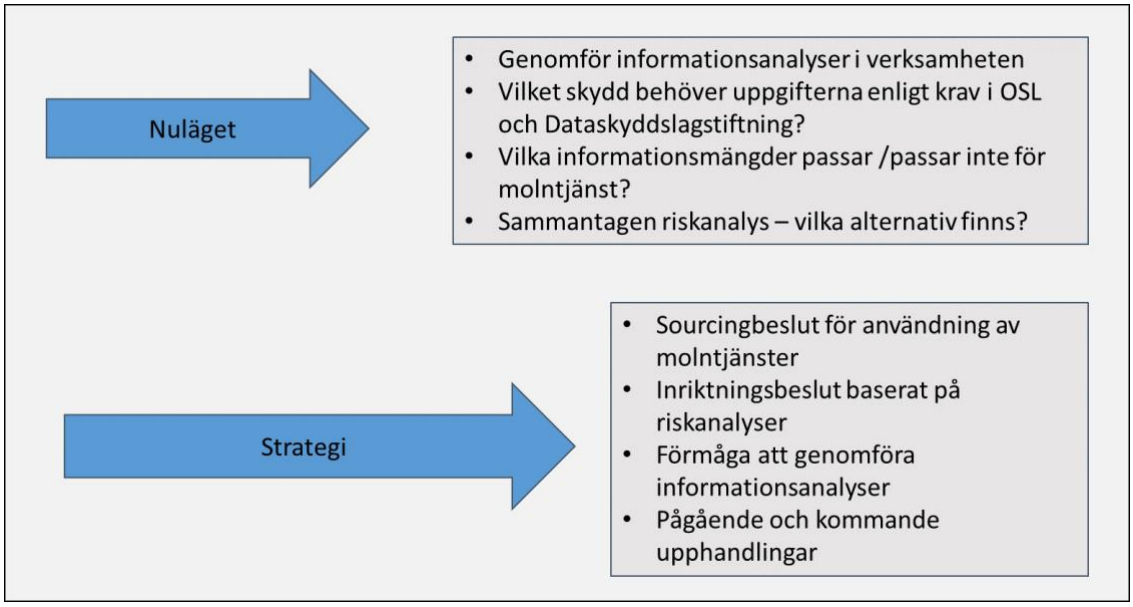
- Hur beroende blir verksamheten av tjänsten och vilken möjlighet finns att kontrollera hur informationen hanteras?
- Hur kan man säkerställa ägarskapet av informationen för att till exempel kunna ta tillbaka information vid byte till ny leverantör – hur ”fastlåst” blir man?

Behovet att hantera nuläget kan dock medföra andra vägval och beslut än vad som är möjligt eller önskvärt ur ett strategiskt långsiktigt perspektiv.

I de kommuner och regioner där omställning till molntjänster och nya arbetssätt redan är genomförd, där det finns äldre it-miljö (legacy) som inte längre kan nå upp till verksamhetens krav och inom områden med begränsad konkurrens kan alternativen vara begränsade. I dessa fall bör ett beslut om användning av

molntjänst fattas efter en sammanvägd och riskbaserad bedömning som även bör dokumenteras.

SKLs vägledning om molntjänster och rättsliga frågor är främst avsedd att ge stöd för att kunna hantera nuläget och de analyser som behöver genomföras.



Sammanfattning av rättsliga frågor

Statlig utredning

Regeringen har den 26 september 2019 beslutat att tillsätta en statlig utredning Säker och kostnadseffektiv it-drift för den offentliga förvaltningen (Dir. 2019:64). I utredningens uppdrag ingår att utreda rättsliga förutsättningar för utkontraktering till privata leverantörer, frågor om krav på hantering av sekretesskyddade uppgifter och risk för röjande, analys av regelverket kring dataskydd särskilt vad gäller behandling av känsliga personuppgifter med flera frågor.

Utredaren ska också särskilt analysera eventuella konsekvenser av att uppgifter som lämnas ut till en privat leverantör kan komma att exponeras för andra staters rättsordningar. Särskilt fokus ska ligga på betydelsen av rättsakter från tredjeland, t ex amerikanska CLOUD Act.

Utredningen ska lämna förslag i denna del den 31 augusti 2020.

Läs SKLs kommentar till utredningen.

Dataskydd

Behandling av personuppgifter får bara ske när det finns lagligt stöd i dataskyddslagstiftningen (GDPR) och om uppgifter ska lämnas ut till ett land utanför EU/EES-området krävs att vissa förutsättningar är uppfyllda. Precis som för uppgifter som omfattas av sekretess bygger regelverket på att personuppgiftsansvarig gör en aktiv bedömning inför utlämnandet.

Vid användning av molntjänster där flera olika typer av uppgifter kommer att hanteras blir det nödvändigt att kunna göra en bredare schablonbedömning och utgå från att skydd måste finnas för de mest känsliga personuppgifterna som kan tänkas hanteras i tjänsten.

Varje kommun och region bör noga analysera om molntjänsteleverantören har antagit EU-kommissionens standardavtalsklausuler eller att företagskoncernen har antagit bindande företagsbestämmelser, så kallade Binding Corporate Rules, (BCR) som har utformats av kommissionen.

EU:s dataskyddsmyndighet (EPDB) har identifierat att utlämning av personuppgifter enligt regelverket i CLOUD Act medför ett osäkert rättsläge, men förhandlingar har inletts mellan EU och USA i bland annat denna fråga.

Detta gör SKL

Mot bakgrund av det osäkra rättsläget samt olika synsätt och tolkningar hos kommuner och regioner bedömer SKL att det inte är möjligt att för närvarande lämna generella inriktningsrekommendationer utöver den vägledning som ges i dessa dokument. Det lämnas till enskilda kommuner och regioner att utifrån sina förutsättningar och möjligheter göra sin egen sammantagna riskbedömning.

Detta är långt ifrån tillfredsställande, och därför avser SKL att fortsätta arbeta aktivt med strategisk intressebevakning av området.

SKL samarbetar med SKL Kommentus AB och Inera AB i de parallella projekt som bedrivs. Inom SKL Kommentus AB drivs dialog med molntjänsteleverantörer, ramavtal och avtalsvillkor för tjänsterna, inom Inera AB genomförs en fördjupad undersökning av säkerhetskrav kopplat till olika informationsmängder vid implementering av en molntjänst.