Molntjänster och konfidentialitetsbedömning

EN VÄGLEDNING TILL KOMMUNER OCH REGIONER I ARBETET ATT UTVECKLA VERKSAMHET MED DIGITALISERING V1.1 20191105

Sveriges Kommuner och Landsting

Innehållsförteckning

En modell som stöd

Molntjänster kan effektivisera arbetet och göra information mer tillgänglig men ändå öka informationssäkerheten för kommuner och regioner. Avgörande för att lyckas är att göra ett medvetet val av molntjänst och hitta rätt typ av tjänst för informationen.

Flera kommuner och regioner har efterfrågat vägledning särskilt när det gäller bedömningen av hur uppgifter som omfattas av sekretess utgör känsliga personuppgifter eller annars är konfidentiella ska kunna hanteras i molntjänster.

Denna vägledning med beskrivning av beslutsprocessen och ett metodstöd ska stödja kommuner och regioner som vill använda molntjänster, särskilt när det gäller konfidentiell information som till exempel omfattas av sekretess eller är känsliga personuppgifter, här sammanfattat som konfidentialitetsbedömning.

Metodstödet innehåller en matrismodell som kan vara till hjälp inför sådana bedömningar, med fokus på konfidentialitet som utgår från den klassificeringsmodell som används inom informationssäkerhet där man normalt beaktar informationens Riktighet, Konfidentialitet och Tillgänglighet[1].

I modellen analyseras inte andra rättsliga frågor eller informationssäkerhetsaspekter, såsom dataskydd, som endast nämns kort, arkivfrågor, allmänna handlingar och tillgänglighet, riktighet och spårbarhet av information. Dessa perspektiv är också är viktiga och för en fullständig analys måste även dessa frågor analyseras inför upphandling och införande av molntjänster. Det innebär att fler regelverk kan aktualiseras som till exempel regler om allmänna handlingar och arkiv med mera. Vissa av dessa frågor berörs i beskrivningen av beslutsprocessen.

Vägledningen är avsedd att fungera som ett stöd för kommunens eller regionens egen analys och beslut och ett förslag är att även dokumentera arbetet och beslutet.

Målgrupp

Modellen kan med fördel användas av en sammansatt grupp där flera kompetenser kan ingå, som till exempel CIO, it-drift-ansvarig, ansvarig för tekniskt it-införande, it-upphandlare, jurist, dataskyddsombud, arkivarie och verksamhetsansvariga.

Genomförande

Denna vägledning för konfidentialitetsbedömning av molntjänster har tagits fram i en arbetsgrupp bestående av experter och sakkunniga inom juridik samt informations- och it-säkerhet inom SKL, SKL Kommentus AB, Inera AB och externa experter och sakkunniga inom juridik samt it- och informationssäkerhet.

Arbetsgruppen har samrått med jurister och sakkunniga vid Danderyds kommun, Fagersta kommun, Falun kommun, Göteborgs stad, Luleå kommun, Region Stockholm, Sundsvalls kommun, Uppsala kommun, Växjö kommun, Inera AB och SKL Kommentus inköpscentral AB, med flera.

Vägledningarna har remitterats i två omgångar och kommuner och regioner har haft tillfälle att lämna synpunkter.

[1] Etablerad modell för informationsklassning finns i Metodstöd för systematiskt informationssäkerhetsarbete, MSB; https://www.informationssakerhet.se/metodstodet/utforma/#utformning-av-matrisen-%E2%80%93-antal-kolumner-och-rader

Vägledningarna om molntjänster är uppdelade i tre delar, förutom denna vägledning om konfidentialitetsbedömning även:

- Molntjänster i verksamheten
  En sammanfattning för verksamhetsansvariga som stöd i arbetet med att utveckla verksamheten med digitalisering
- Fakta-PM om CLOUD Act

Att införa molntjänster

Molntjänster är en övergripande benämning på tjänster som innebär att en leverantör tillhandahåller lagring, datorkapacitet, datorprogram, applikationer, funktioner, plattformar eller liknande lokalt eller i tjänsteleverantörens egna datorhallar med stöd av elektroniska kommunikationsnät. En stark trend är att många applikationer levereras som molntjänst istället för som enskilda installationer i användarnas egna datorer.

Det finns många fördelar med molntjänster. Till exempel att användaren inte särskilt behöver upphandla och investera i egen datorkapacitet eller lagringsutrymme när behov uppstår utan tillgången kan snabbt och lätt justeras efter verksamhetens behov. Tillgängligheten till informationen kan öka genom att möjligheterna till åtkomst ökar med tillgång till informationen med hjälp av till exempel internet. Molntjänster kan även ge ett ökat skydd mot antagonistiska it-säkerhetshot[2] dels genom att mjukvara alltid hålls uppdaterad dels genom att molntjänstleverantören med sin storskaliga verksamhet har möjlighet att avsätta mer resurser för och har högre kompetens om informationssäkerhet i it-system än vad många kommuner och regioner kan ha möjlighet till.

Molntjänster tillhandahålls ofta av internationella företag och information som hanteras av företagen kan i praktiken överföras till och behandlas i många olika länder. Molnleverantören kan lyda under andra länders lagstiftning och tvingas överlämna sina kunders information till brottsbekämpande och andra myndigheter i dessa länder.

Inför användning av molntjänster krävs, precis som vid andra sourcinglösningar, att organisationen analyserar ett antal aspekter för att säkerställa att molntjänsten passar för verksamheten och den information som ska hanteras. Bland de analyser som måste göras finns analys av rättsliga förutsättningar och säkerhet för informationen.

Kommuner eller regioner som inför molntjänster i sin verksamhet bör alltså först genomföra analyser av bland annat verksamhetsbehov och funktionalitet, vilken typ av information som ska hanteras i molntjänsten, ifall det förekommer personuppgifter, att tjänsten och leverantören kan nå upp till säkerhetskraven, vilka alternativa tjänster och leverantörer som finns och en sammantagen behovs- och riskanalys.

Systematiskt informationssäkerhetsarbete och dataskydd

Till stor del är detta motsvarande analyser som behöver genomföras i samband med annan it-upphandling eller vid egen it-drift. De flesta analyserna ingår dessutom i det systematiska informationssäkerhetsarbetet och dataskyddsarbetet som bör finnas inom alla kommuner och regioner.

Inom ramen för ett systematiskt informationssäkerhetsarbete ingår bland annat:

- *Informationsklassning*; Verksamhetens olika informationsmängder ska vara klassificerade för att kunna fastställa rätt nivå av säkerhet.
- *Kravställning av säkerhetsåtgärder*; Klassningen används för att ställa krav inom den egna organisationen på egen it-drift och på administrativa rutiner med mera. Den används också för att kunna ställa krav på leverantörer så att olika typer av information ges rätt skydd. För publika molntjänster med

[2] Det kan till exempel röra sig om dataintrång, tillgänglighetsattacker och utpressningsförsök.

standardiserade villkor genomförs detta omvänt så att molntjänsteleverantören och tjänsten kontrolleras så att nödvändig kravnivå kan verifieras.
- *Uppföljning*; I det systematiska informationssäkerhetsarbetet ska rutiner för uppföljning och kontroll ingå så att det regelbundet kan kontrolleras att skyddet upprätthålls.

Inom ramen för organisationens dataskyddsarbete ingår bland annat:

- *Laglighetsbedömning*; Är det tillåtet enligt dataskyddslagstiftningen (GDPR) eller annan integritetsskyddande lagstiftning, t.ex. offentlighets- och sekretesslagen (OSL) att behandla uppgifterna så som är avsett och att även använda den typ av behandling som molntjänsten innebär?
- *Konsekvensbedömning*; Om en behandling av personuppgifter sannolikt leder till en hög risk för enskilda personers fri- och rättigheter ska enligt art. 35 GDPR en konsekvensbedömning[3] genomföras och den ska utgå från en riskanalys.

Publika molntjänster[4]

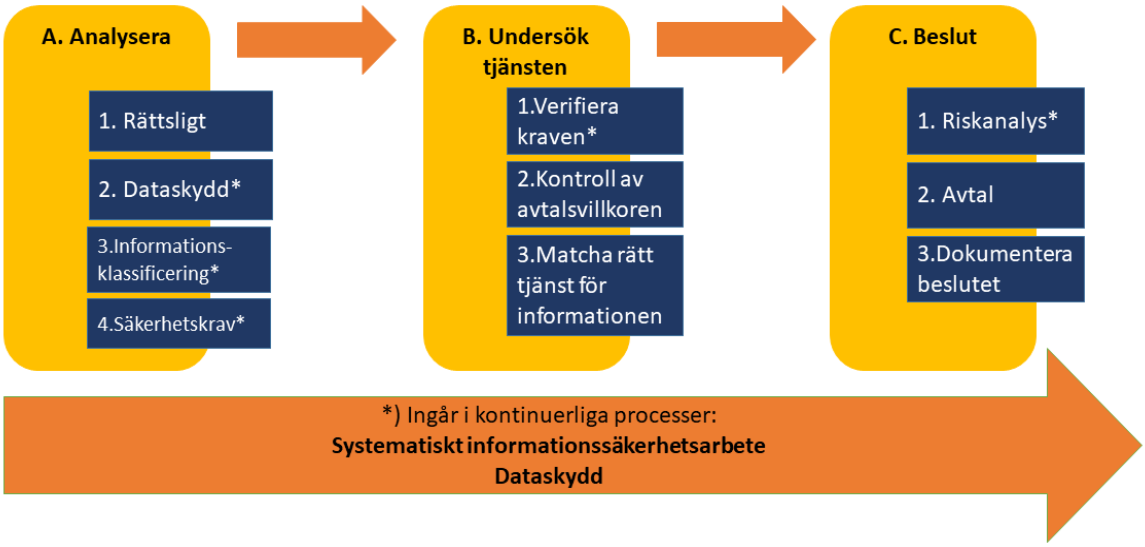
När det gäller molntjänsteleverantörer med utländskt ägande och global verksamhet som tillhandahåller publika molntjänster med standardiserade villkor, tillkommer aspekter i analyserna. Man behöver då undersöka hur säkerheten ser ut för den specifika lösningen, hur informationen behandlas då den transporteras och i vilken mån informationen hålls åtskild, vilka som har tillgång till den och var den lagras geografiskt, samt vilket lands lagstiftning som gäller vid krav på utlämnande av information.[5] Ibland kan säkerheten vad avser konfidentialitet, tillgänglighet, riktighet och spårbarhet bli avsevärt högre vid användning av molntjänster. Men samtidigt kan det finnas krav eller funktionalitet i molntjänsten som gör att konfidentialitet inte kan upprätthållas i förhållande till den aktuella molntjänstleverantören.

Denna vägledning är avsedd att vara ett stöd för de delar av analysarbetet som tar sikte på om konfidentiell information kan behandlas inom ramen för denna typ av molntjänster.

[3] Information om konsekvensbedömning, se Datainspektionen; https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/konsekvensbedomningar-och-forhandssamrad/vem-maste-gora-en-konsekvensbedomning/

[5] Molntjänster i staten, Pensionsmyndigheten, s. 17.

Beslutsprocess inför användning av molntjänst



A. Analysera

1. Rättsligt

De rättsliga förutsättningarna för informationshanteringen ingår till viss del i informationssäkerhets- och dataskyddsarbetet, men inför användning av molntjänster kan det även vara bra att undersöka om det finns annan reglering som kan påverka och t.ex. ge vissa formkrav eller påverka funktionalitet i tjänsten. För alla myndigheter ställs särskilda krav på hanteringen av allmänna handlingar, möjligheten att kunna hålla dessa ordnade enligt arkivbestämmelser, kunna radera vid gallring, återta information och kunna flytta över till annan tjänst utan att förlora den.

Det ställs även krav på att uppgifter som omfattas av sekretess kan skyddas.

Läs mer om rättsliga frågor i nästa kapitel i denna vägledning.

2. Dataskydd

Dataskyddslagstiftningen (GDPR) ställer krav på att all behandling av personuppgifter ska ha stöd i lag, hanteras enligt regelverket och ges lämpligt skydd. Vid alla avtal med leverantörer som ska behandla personuppgifter åt kommunen eller regionen, krävs ett personuppgiftsbiträdesavtal[6].

Vid användning av globala molntjänster aktiveras bestämmelserna om överföring till tredje land och det finns krav på att det land dit uppgifterna ska överföras till antingen har godkänd dataskyddslagstiftning eller att leverantören följer särskilda villkor från EU. Det är kommunens eller regionens ansvar att se till att teckna ett biträdesavtal och kontroller att rätt avtalsvillkor finns.

[6] SKL har tagit fram en mall personuppgiftsbiträdesavtal

Läs mer om SKLs rättsliga frågor och samråd med organisationens dataskyddsombud (DSO) för att få stöd i bedömningen.

3. Informationsklassificering

Det finns ett flertal vägledningar som är till hjälp i det kontinuerliga arbetet med informationssäkerhet. MSB har ett metodstöd för systematiskt informationssäkerhetsarbete som bland annat inkluderar hur man kan gå till väga för att bland annat göra:

- omvärldsanalys,
- verksamhetsanalys och
- riskanalys.[7]

Dessa verktyg blir utgångspunkt för att förtydliga vilket skydd informationen behöver och vilka krav som en molntjänst behöver klara. I dessa ingår en matris för informationsklassificering som bygger på etablerade standarder.

SKL har ett verktyg för att förenkla kommuners och regioners arbete med informationsklassning av verksamhetssystem och datalagring (KLASSA).[8]

KLASSA och metodstödet för systematiskt informationssäkerhetsarbete bygger på standarden SS-EN ISO/IEC 27001.

Det rekommenderas att de olika informationstyper som blir aktuella i en molntjänst har klassats så att det är tydligt för organisationen hur skyddsvärd informationen är ur olika perspektiv. I nästa kapitel finns en matris som ger stöd för att genomföra konfidentialitetsbedömningen med avseende på just informationshantering i globala molntjänster.

4. Säkerhetskrav

Med utgångspunkt från analyserna ovan ska säkerhetsåtgärder väljas så att informationen kan ges rätt nivå av skydd[9].

För en publik molntjänst med standardiserade villkor måste de säkerhetskrav som annars skulle ställas i en upphandling istället kontrolleras mot tjänstens funktionalitet och avtal. Detta kan vara ett omfattande arbete eftersom flera globala molntjänsteleverantörer har komplexa avtalspaket och tjänsten kan implementeras på flera olika sätt.

Ett vanligt krav kan gälla kryptering, som kan införas på olika sätt med olika typer av nyckelhantering.

[7] https://www.informationssakerhet.se/metodstod-for-lis/.
[8] https://klassa-info.skl.se/.
[9] Mer om säkerhetskrav se;
https://skl.se/naringslivarbetedigitalisering/digitalisering/arkitektursakerhet/informationssakerhet/informationssakerhetochoutsourcing.12984.html

A. Undersök tjänsten

1. Verifiera kraven

I den här fasen behöver man ofta arbeta iterativt och gå tillbaka till föregående fas (A.4) för att undersöka hur olika införandealternativ kan möta informationsklassningen och säkerhetskraven och vilken påverkan de olika alternativen får för funktionalitet och verksamhet.

2. Kontroll av avtalsvillkoren

Vilken typ av information ska hanteras i en molntjänst och hur beroende verksamheten blir av tjänsten kan avgöra hur stor vikt som läggs vid granskning av avtalsvillkoren. Vid publika molntjänster finns liten eller ingen möjlighet att modifiera villkoren utan det blir en fråga om att matcha informationen med en lämplig molntjänst och acceptera de villkor som finns.

Vissa saker måste dock verifieras, att det finns personuppgiftsbiträdesavtal, att leverantören har accepterat EU:s standardiserade villkor, att leverantören inte har rätt att ta del av informationen utan kundens insyn och kontroll och att möjlighet finns till kontroll av underleverantörer med mera.[10]

3. Matcha rätt tjänst för informationen

Sammantaget blir kontrollerna och analyserna som beskrivs ovan ett stöd för att kunna välja en molntjänst som är lämplig för den typ av information som ska hanteras i den. I praktiken blir valet också ett val mellan de olika alternativ som står till buds. När det finns få alternativ blir vikten av arbetet med kontroll ännu större så att de säkerhetsmekanismer som är möjliga att genomföra också används.

B. Beslut

1. Riskanalys

I den sammantagna riskanalysen vägs det underlag som har tagits fram genom kontrollerna mot de risker som finns med molntjänsten. I en undersökning har Örebro Universitet på uppdrag av MSB[11] undersökt molntjänster och beskriver risker ur flera perspektiv. Riskanalysen behöver även omfatta risker med de tillgängliga alternativ som finns istället för den aktuella molntjänsten. Riskanalysen ska fungera som stöd för beslut.

Artikel 35.1 i dataskyddsförordningen (GDPR) beskriver hur personuppgiftsansvariga ska genomföra en så kallad dataskyddskonsekvensbedömning[12] om en personuppgiftsbehandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter (konsekvensbedömning). Syftet med en konsekvensbedömning är att förebygga risker för registrerades personliga integritet innan de uppkommer.

Konsekvensbedömningen är en process för att

[10] För ett exempel på vilka villkor som bör granskas se Utredning Office 365 i Danderyds kommun, fastställd den 30 september 2019, Kommunstyrelsen Danderyds kommun (Dnr. KS 2019/0296). Notera att utredning och beslut är genomförd efter Danderyds förutsättningar och att varje organisation behöver avgöra sin förmåga att etablera it-säkerhet och ställa mot de villkor och möjligheter som leverantör och tjänst erbjuder.

[11] Säkerhet vid molnlösningar, 2018; https://www.msb.se/sv/publikationer/sakerhet-vid-molnlosningar-studie/

[12] Mer information om konsekvensbedömningar finns på www.datainspektionen.se.

• ta reda på vilka risker som finns med att behandla personuppgifter

• ta fram rutiner och åtgärder för att reducera eller eliminera dessa risker och

• visa för registrerade, samarbetspartners eller tillsynsmyndighet att man uppfyller dataskyddsförordningens krav.

En dokumenterad konsekvensbedömning går längre än en riskanalys på så sätt att den, förutom en riskanalys också ska beakta åtgärder för att reducera eller eliminera risker samt en sammantagen bedömning av om hög risk för enskildas fri- och rättigheter vid personuppgiftsbehandling kvarstår. Kvarstår en hög risk, trots tekniska och organisatoriska kompensatoriska åtgärder, kan den personuppgiftsansvarig välja att antingen begära förhandssamråd hos Datainspektionen eller avstå från den bedömda molntjänsten.

2. Avtal

När beslutet är fattat kan avtal tecknas.

3. Dokumentera beslutet

Av flera skäl är det viktigt att dokumentera analyserna och beslut om användning av molntjänst. Inte minst är det nödvändigt enligt dataskyddsförordningen att kunna informera om personuppgiftsbehandling över tid.

Metodstöd för bedömning av konfidentialitet

1		2	3	4	5
Exempel på uppgifter av olika grad av känslighet	**Konsekvensnivåer vid förlust av konfidentialitet**	**Förekommer uppgifter som omfattas av säkerhetsskyddslagen?**	**Förekommer sekretessreglerade uppgifter?**	**Molntjänstjänsteleverantören har säte/ är registrerat/ huvudkontor i annat land?**	**Förekommer personuppgifter i tjänsten?**
Uppgifter om totalförsvar, relationer med andra länder	Kan röjande innebära konsekvenser för Sverige säkerhet?	Är svaret ja? Uppgifterna bör inte behandlas i en molntjänst	Ja, eller säkerhetsskyddad verksamhet	Molntjänster bör inte användas	N/A
Sekretess, känsliga personuppgifter	Allvarlig eller katastrofal negativ påverkan på egen eller annan verksamhet och dess tillgångar, eller för enskild individ.	N/A	Ja, är det möjligt att göra leverantören behörig? Är det möjligt att tillämpa avtalsmässig tystnadsplikt? Är det möjligt att skydda informationen genom kryptering?	Molntjänster bör som försiktighetsprincip inte användas. Kryptering kan undersökas om det kan fungera som skydd. Myndigheten bör göra en samlad riskbedömning om den ändå går vidare med leverantören.	Överförs personuppgifter till tredje land? Kapitel V i GDPR
Uppgifter om upphandling	Betydande negativ påverkan på egen eller annan verksamhet och dess tillgångar, eller för enskild individ.	N/A	Se ovan.	Om sekretessen endast är avsedd för att skydda den egna verksamheten, kort sekretesstid. Skulle kunna använda molntjänst efter en samlad riskbedömning.	Överförs personuppgifter till tredje land? Kapitel V i GDPR
Uppgifter som inte omfattas av sekretess, är särskilt skyddsvärda personuppgifter eller personuppgifter som inte är känsliga.	Måttlig negativ påverkan på egen eller annan verksamhet och dess tillgångar, eller för enskild individ.	N/A	Molntjänster bör kunna användas, Är det lämpligt?	Molntjänster bör kunna användas, Är det lämpligt?	Överförs personuppgifter till tredje land? Kapitel V i GDPR
Öppen och offentlig information	Försumbar eller ingen negativ inverkan på egen eller annan verksamhet eller för enskild individ	N/A	Molntjänster bör kunna användas, Är det lämpligt?	Molntjänster bör kunna användas, Är det lämpligt?	Överförs personuppgifter till tredje land? Kapitel V i GDPR

Figur 1 Matris som syftar till att ge en överblick och stöd i analysarbetet, en större bild finns på sidan 15.

1. Analysera informationen

Vilken information ska hanteras i molntjänsten?

Genom kartläggningen av verksamheten kan kommunen eller regionen få en uppfattning om vilka typer av informationstillgångar som kan komma att hanteras i molntjänsten. Med denna kunskap bör kommunen eller regionen därefter bedöma hur skyddsvärd informationen är ur ett individ-, verksamhets- och samhällsperspektiv för att kunna bedöma om det över huvud taget är lämpligt att hantera informationen i en molntjänst. I detta arbete ingår bland annat informationsklassning och riskanalys, se till exempel KLASSA och MSB:s metodstöd för systematiskt informationssäkerhetsarbete.

När kommunen eller regionen därefter vet vilken typ av information som ska hanteras måste den ta ställning till vilka rättsregler som är tillämpliga i till exempel OSL, dataskyddsförordningen eller särskild registerförfattning.

Vilka legala krav på konfidentialitet som ställs när uppgifter från kommuner eller regioner ska hanteras i en molntjänst beror bland annat på vilken typ av information rör sig om. När kommunen eller regionen ska kontrollera lagligheten av hanteringen av information i en molntjänst bör kommunen eller regionen redan ha bestämt vad som är syftet med att hantera informationen i den tänkta tjänsten och vilka funktioner kommunen eller regionen eftersträvar i tjänsten.

Alla kommuner eller regioner som anlitar en molntjänstleverantör, för att bearbeta, lagra eller på annat sätt hantera kommunens eller regionens information måste pröva om det är tillåtet att lämna ut informationen till leverantören i fråga och analysera vilka eventuella konsekvenser ett utlämnande kan få. Utlämnandet måste vara förenligt med gällande sekretesslagstiftning.

För att kunna avgöra om det är lagligt eller lämpligt att anlita en molntjänstleverantör för en viss tjänst måste det med andra ord vara känt vem eller vilka som hanterar informationen, hur informationen hanteras samt var den befinner sig geografiskt

2. Förekommer uppgifter som omfattas av säkerhetsskydd?

Omfattas informationen av säkerhetsskydd eller annan sekretess?

När kommunen eller regionen har kartlagt innehållet i informationen blir nästa steg att analysera om informationen omfattas av Säkerhetsskyddslagen (2018:585), SSL och om informationen innehåller uppgifter som är sekretessreglerade i Offentlighets- och sekretesslagen (2009:400), OSL.

Uppgifter om säkerhetskyddsklassade verksamheter och uppgifter som är säkerhetsskyddsklassade bör inte hanteras i molntjänster eftersom det vore mycket problematiskt att teckna säkerhetsskyddsavtal med en internationell molntjänstleverantör och genomföra en säkerhetsprövning av anställda som är utländska medborgare och som har sin

arbetsplats utanför Sveriges gränser. Att hantera information som omfattas av säkerhetsskyddslagen i en publik molntjänst bör därmed som huvudregel vara uteslutet.

Om det rör sig om enstaka uppgifter som omfattas av sekretess kan kommunen eller regionen fundera över om det är möjligt att hantera dessa uppgifter på ett annat sätt och därigenom möjliggöra att använda molntjänsten för större delen av informationstillgångarna.

3. Förekommer uppgifter som omfattas av sekretess?

Är det möjligt att göra anställda hos leverantören behörig att ta del av uppgifterna?

Ett sätt att möjliggöra användningen av en molntjänst kan vara att säkerställa att endast en eller ett par särskilt utpekade anställda hos leverantören får arbeta med kommunens eller regionens informationstillgångar. Dessa personer knyts till kommunen eller regionen genom särskilda förordnanden så att de anses delta i verksamheten på lika villkor som kommunen eller regionens egna anställda och under samma arbetsledning. De kan därmed göras behöriga att ta del av den sekretessbelagda informationen. Något röjande i OSL:s mening sker då inte när dessa personer arbetar med tjänsten inom ramen för sina behörigheter. Ibland är det dock inte lämpligt eller möjligt att göra anställda hos en leverantör behörig på detta sätt, exempelvis vad avser enskilda anställda som utför arbetet från ett annat land, samtidigt som de bor och arbetar i det andra landet.

Är det möjligt med avtalsreglerad tystnadsplikt?

Under vissa förhållanden kan en avtalsreglerad tystnadsplikt medföra att informationen kan lämnas ut till molntjänstleverantören. Ett sådant avtal förutsätter att de enskilda arbetstagare hos molntjänstleverantören som får tillgång till informationen har avtalsmässig tystnadsplikt i förhållande till kommunen eller regionen

Är det möjligt att kryptera informationen?

Om kommunen eller regionen krypterar informationen innan den överlämnas till molntjänstleverantören kan uppgifterna inte anses röjda för leverantören och bör kunna lämnas ut i krypterad form. Eftersom uppgifter om kryptering är sekretessbelagda uppgifter kan dessa uppgifter inte lämnas ut till en molntjänstleverantör utan att uppgiften ska anses röjd. Syftet med att lämna ut en krypteringsnyckel till en molntjänstleverantör är att leverantören ska använda den. För att säkerställa ett godtagbart skydd för övriga sekretessbelagda uppgifter bör kommunen eller regionen behålla krypteringsnyckeln.

Det förekommer att leverantörer av molntjänster tillhandahåller olika lösningar för kryptering antingen med molntjänstleverantörens egna kryptonyckel eller att kunden, det vill säga kommunen eller regionen använder en egen kryptonyckel. Beroende på vad det är för molntjänst kan uppgifterna hanteras på olika sätt av molntjänstleverantören, exempelvis genom lagring, överföring eller under bearbetning. När uppgifter är under bearbetning måste de i dagsläget som regel vara dekrypterade och kan därför finnas tillgängliga för en molntjänstleverantör i läsbar form.

Informationens status[1]	Nyckel[2]	Egen kryptonyckel		Molntjänstleverantörens kryptonyckel	
		Rättsligt	Funktionellt	Rättsligt	Funktionellt
Lagring		Ja[3]	OK	Nej[4]	OK
Överföring		Ja[3]	OK	Nej[4]	OK
Bearbetning		Ja[3]	Inte OK	Nej[4]	OK

1. Informationen som lagras befinner sig i vila, informationen överförs när den sänds mellan olika platser, informationen bearbetas när en eller flera personer aktivt öppnat eller skriver i ett dokument.
2. Nyckel är information som krävs för att kunna ta del av krypterad information i läsbar form. Med egen kryptonyckel säkerställs att ingen obehörig kan komma åt informationen.
3. Genom kryptering och exklusiv tillgång till nyckeln säkerställs att ingen obehörig kan ta del av uppgifterna. För viss information kan det finnas rättsliga krav på kryptot.
4. Uppgift om kryptonyckel omfattas av sekretess och obehöriga får inte ta del av sådana uppgifter. Att enbart använda molntjänstleverantörens nyckel är som kommunen eller regionen inte krypterar uppgifterna. För vissa typer av uppgifter, exempelvis personuppgifter torde det som regel krävas kryptering som säkerhetsåtgärd.

Figur 2 Matris över möjligheterna till kryptering i olika situationer och hur det kan förhålla sig till molntjänstens funktionalitet.

Som framgår av figur 5 kan det i vissa fall finnas svårigheter med att använda kryptering där enbart kommunen eller regionen har tillgång till krypteringsnyckeln eller att använda tjänsterna med bibehållen/önskad funktionalitet.

4. Har molntjänstleverantören anknytning till annat land

Exponeras informationen för andra länders rättsordningar?

Kommunen eller regionen behöver också ta hänsyn till om det finns andra omständigheter som talar för att det är olämpligt att lämna ut informationen till molntjänstleverantören. En sådan omständighet kan vara att informationen exponeras för andra länders rättsordningar om den lagras utanför Sveriges gränser eller om utländsk rättsordning som träffar molntjänstleverantören medför att uppgiften kan komma att lämnas ut även om uppgifterna lagras i Sverige. Informationen blir därmed potentiellt tillgänglig för till exempel andra länders myndigheter.

Om uppgifterna omfattas av sekretess och informationen potentiellt kan bli tillgänglig för andra länders myndigheter synes en tolkning vara att molntjänster i praktiken inte kan användas för att behandla eller lagra dessa uppgifter, oavsett om uppgifterna krypteras.[13] Å andra sidan tyder viss praxis på att uppgifter i sig inte ska anses röjda även om de lämnas ut till obehöriga i ett annat land, jfr AD 2019 nr 15.

Riskanalys

Om kommunen eller regionen ändå har ett starkt behov och intresse av att använda molntjänsten bör en riskanalys genomföras för att avgöra om det trots att uppgifterna exponeras för en utländsk rättsordning ändå inte är olämpligt att molntjänsten används. Så skulle till exempel kunna vara fallet om sekretessen endast gäller för en kortare tid eller det inte är sannolikt att uppgifterna kan komma att begäras ut inom ramen för en utländsk straffprocess för vilken molntjänstleverantören är exponerad eller liknande.

[13] Rättsligt uttalande om röjande och molntjänster, eSam, 2018-10-23, VER 2018:57.

Kommunen eller regionen behöver även göra en riskavvägning som jämför olika alternativ till molntjänsten. Riskanalysen behöver väga organisationens egna förutsättningar och förmåga att upprätthålla it-säkerhet i t.ex. egen it-drift mot de möjligheter och risker som molntjänsten innebär samt den påverkan som leverantörens villkor utgör.

I MSB:s metodstöd för systematiskt informationssäkerhetsarbete finns vägledning bland annat för hur riskanalyser kan göras.[14]

Där ges bl.a. exempel på kriterier för konsekvens- och sannolikhetsbedömning:

- Ekonomisk förlust
- Påverkan på eller avbrott i verksamheten
- Överträdelse av regelkrav
- Minskat förtroende
- Skada på annan organisation eller samhället
- Personskada

Det finns även exempel på kriterier för riskacceptans:

- Vid vilken nivå av sannolikhet risker kan accepteras
- Vid vilken nivå av konsekvenser kan risker accepteras

5. Förekommer personuppgifter?

Förekommer personuppgifter bland informationstillgångarna?

Om personuppgifter kommer att förekomma i molntjänsten måste dataskyddsförordningens regler alltid beaktas oavsett om uppgifterna omfattas av sekretess eller inte. Den personuppgiftsansvariga måste fortlöpande kunna säkerställa konfidentialitet hos behandlingsystem och -tjänster, (art 32 dataskyddsförordningen). Om behandlingen med beaktande av dess art, omfattning sammanhang och ändamål leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige före behandlingen göra en konsekvensbedömning, art 35.1 dataskyddsförordningen.

Det kan dels kan det behöva upprättas ett personuppgiftsbiträdesavtal med molntjänstleverantören dels måste det klargöras om personuppgifterna kan komma att föras över till tredje land. Om uppgifterna kan komma att föras över till tredje land måste en bedömning göras om överföringen eller överföringarna är förenliga med dataskyddsförordningen. I förhållande till personuppgifter spelar det ingen roll om uppgifterna är krypterade vid överföringen till tredje land. En överföring av krypterade personuppgifter får inte göras om det inte finns ett kommissionsbeslut rörande landet eller något annat undantag enligt kap. V i dataskyddsförordningen kan tillämpas.

[14] https://www.informationssakerhet.se/metodstod-for-lis/identifiera-och-analysera/.

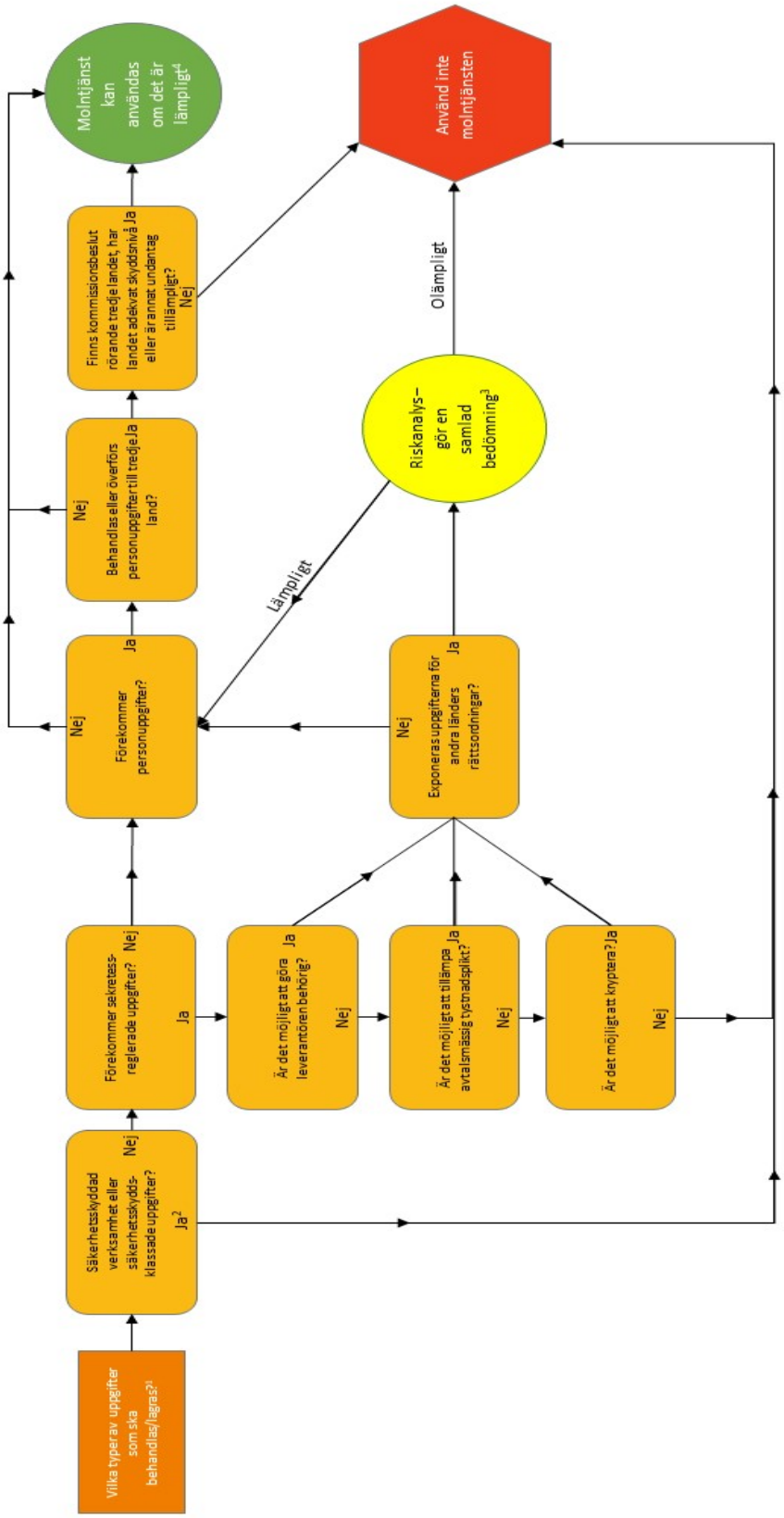
Lämplighetsbedömning

Även om det inte finns något rättsligt hinder mot att använda en viss molntjänst bör kommunen eller regionen ändå fundera över om det ändå är lämpligt ur ett konfidentialitetsperspektiv att använda molntjänsten. Det kan gälla för information som inte omfattas av sekretess men där en riskanalys visar att informationen skulle kunna vara extra känslig av andra skäl, till exempel elevarbeten med reseberättelser eller liknande från konfliktområden eller andra texter.

Vägledningsmatris och flödesschema

Som stöd för analysarbetet med avseende på konfidentialitet när myndigheter överväger att upphandla en molntjänst för delar av sin it-verksamhet eller it-miljö kan matrisen i bilaga 1 eller flödesschemat i bilaga 2 användas.

Analysera informationen		Förekommer uppgifter som omfattas av säkerhetsskydd?	Förekommer sekretess-reglerade uppgifter?	Har molntjänstleverantören anknytning till ett annat land?	Förekommer personuppgifter?
Exempel på uppgifter av olika grad av känslighet	**Konsekvensnivåer vid förlust av konfidentialitet**	**Förekommer uppgifter som omfattas av säkerhetsskyddslagen?**	**Förekommer sekretessreglerade uppgifter?**	**Molntjänstjänsteleverantören har säte/ är registrerat/ huvudkontor i annat land?**	**Förekommer personuppgifter i tjänsten?**
Uppgifter om totalförsvar, relationer med andra länder	Kan röjande innebära konsekvenser för Sverige säkerhet?	Är svaret ja? Uppgifterna bör inte behandlas i en molntjänst	Ja, eller säkerhetsskyddad verksamhet	Molntjänster bör inte användas	N/A
Sekretess, känsliga personuppgifter	Allvarlig eller katastrofal negativ påverkan på egen eller annan verksamhet och dess tillgångar, eller för enskild individ.	N/A	Ja, är det möjligt att göra leverantören behörig? Är det möjligt att tillämpa avtalsmässig tystnadsplikt? Är det möjligt att skydda informationen genom kryptering?	Molntjänster bör som försiktighetsprincip inte användas. Kryptering kan undersökas om det kan fungera som skydd. Myndigheten bör göra en samlad riskbedömning om den ändå går vidare med leverantören.	Överförs personuppgifter till tredje land? Kapitel V i GDPR
Uppgifter om upphandling	Betydande negativ påverkan på egen eller annan verksamhet och dess tillgångar, eller för enskild individ.	N/A	Se ovan.	Om sekretessen endast är avsedd för att skydda den egna verksamheten, kort sekretesstid. Skulle kunna använda molntjänst efter en samlad riskbedömning.	Överförs personuppgifter till tredje land? Kapitel V i GDPR
Uppgifter som inte omfattas av sekretess, är särskilt skyddsvärda personuppgifter eller personuppgifter som inte är känsliga.	Måttlig negativ påverkan på egen eller annan verksamhet och dess tillgångar, eller för enskild individ.	N/A	Molntjänster bör kunna användas, Är det lämpligt?	Molntjänster bör kunna användas, Är det lämpligt?	Överförs personuppgifter till tredje land? Kapitel V i GDPR
Öppen och offentlig information	Försumbar eller ingen negativ inverkan på egen eller annan verksamhet eller för enskild individ	N/A	Molntjänster bör kunna användas, Är det lämpligt?	Molntjänster bör kunna användas, Är det lämpligt?	Överförs personuppgifter till tredje land? Kapitel V i GDPR



1. I detta arbete ingår att klassificera informationen, jfr SKL:s verktyg KLASSA.
2. Om inte säkerhetsskyddad upphandling genomförs.
3. Se SKL:s vägledning - Molntjänster och konfidentialitetsbedömning för sekretessinformation och personuppgifter, avsnitt 3.3.5. Stöd i riskanalysarbetet kan även hittas på https://www.informationssakerhet.se/metodstod-for-lis/identifiera-och-analysera/.
4. Se SKL:s vägledning - Molntjänster och konfidentialitetsbedömning för sekretessinformation och personuppgifter, avsnitt 3.5.