Vägledning för socialtjänsten vid användning av molntjänster

Sveriges Kommuner och Regioner

Utbudet av molnbaserade digitala tjänster för socialtjänsten är inte stort, men ökar. Det finns flera fördelar med molntjänster. Skalbarheten är en sådan, dvs. man betalar för den kapacitet man behöver. En annan fördel är priset eftersom flera användare delar på samma resurser. Leverantörerna av molntjänster lägger vidare stor vikt vid skyddet av uppgifter och har ofta expertkunnande inom området.

Det finns också risker med molntjänster. Det ligger i sakens natur att när en myndighet utkontrakterar vissa arbetsuppgifter, t.ex. teknisk bearbetning eller lagring av personuppgifter, till en leverantör så tappar myndigheten samtidigt en del av den faktiska kontrollen över arbetsuppgifterna. Att anlita utländska leverantörer med säte eller datacenter i ett annat land kan försvåra inte bara kontrollen över data, utan också möjligheten att driva effektivt en civilrättslig eller straffrättslig process mot leverantören eller dess medarbetare, t.ex. vid brister i tjänsten eller återkrav på skadestånd som utgivits till registrerade på grund av leverantörens försumlighet.

Det finns också juridiska risker som måste beaktas, bl.a. lagstiftning som leverantören är skyldig att följa och som kan innebära att denne kan tvingas lämna ut kundens personuppgifter på begäran av en domstol eller myndighet i hemlandet, och därtill med yppandeförbud mot kunden. Det finns också krav på skydd i svenska författningar som socialnämnden och leverantören måste iaktta och som har bäring på molntjänster, t.ex. att överföringen av känsliga personuppgifter mellan molntjänst och lokalt system måste vara krypterad.

Många av de risker som är förenade med användning av molntjänster kan drabba de individer som är föremål för socialtjänstens insatser och vars uppgifter hanteras i tjänsten. Det rör sig ofta om känsliga eller andra integritetskänsliga personuppgifter som kan få allvarliga negativa konsekvenser för individerna om de kommer i orätta händer, t.ex. vid brister i skyddet av uppgifterna.

I det följande lämnas några rekommendationer för verksamheter inom socialtjänsten som överväger att använda eller upphandla en molntjänst. Rekommendationerna syftar till att uppmärksamma och fånga in risker för en molntjänst som ska vägas in i den sammantagna bedömningen att använda eller upphandla tjänsten.

Det erinras att varje molntjänst är unik. Riskbilden kan därmed skilja sig åt väsentligen mellan olika tjänster. Av SKR:s ställningstagande om informationshantering i molntjänster (länk) framgår bl.a. att kommuner och regioner rekommenderas att noga analysera risker, särskilt för information av känslig karaktär som kan omfattas av sekretess, i samband med informationshantering i molntjänst som kontrolleras av ägare i annat land.

Ta gärna del av SKR:s vägledningar för att analysera frågor om juridik och säkerhet för molntjänster (länk)

Sektionen för socialtjänst, SKR

1. Dataskyddskonsekvensbedömning

Av artikel 35.1 i dataskyddsförordningen följer att den personuppgiftsansvarige ska utföra en dataskyddskonsekvensbedömning om en typ av behandling *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

- 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.

Det är den personuppgiftsansvarige som ansvarar för att genomföra en konsekvensbedömning, dvs. socialnämnden (motsvarande) eller den privata utföraren. Personuppgiftsansvarig är en juridisk eller fysisk person som ensam eller tillsammans med andra bestämmer ändamålen med eller medlen för en viss behandling av personuppgifter. Av förordningen (2001:637) om behandling av personuppgifter inom socialtjänsten följer att socialnämnden (motsvarande) respektive privata utförare är personuppgiftsansvariga för sin respektive personuppgiftsbehandling.

En dataskyddskonsekvensbedömning 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 om huruvida 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 begära förhandssamråd hos Datainspektionen eller avstå från behandlingen.

1.1. När krävs en konsekvensbedömning?

Det inte obligatoriskt att utföra en konsekvensbedömning för varje behandling av personuppgifter. Av GDPR framgår att en konsekvensbedömning krävs om en viss typ av behandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter (artikel 35.1 och skäl 84 dataskyddsförordningen).

En konsekvensbedömning krävs enligt dataskyddsförordningen särskilt i följande fall:

a) Vid en systematisk och omfattande bedömning av fysiska personers personliga aspekter som grundar sig på automatisk behandling, inbegripet profilering, och på vilken beslut grundar sig som har rättsliga följder för fysiska personer eller på liknande sätt i betydande grad påverkar fysiska personer.

b) Vid en behandling i stor omfattning av särskilda kategorier av uppgifter, som avses i artikel 9.1 (ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning), eller av personuppgifter som rör fällande domar i brottmål och överträdelser.

c) Systematisk övervakning av en allmän plats i stor omfattning.

Enligt artikel 35.4 i dataskyddsförordningen ska respektive nationell tillsynsmyndighet upprätta och offentliggöra en förteckning över behandlingar som kräver en konsekvensbedömning. Datainspektionen har, med ledning av riktlinjer från Europeiska dataskyddsstyrelsen, EDPB, publicerat en förteckning över när en konsekvensbedömning ska göras och som kompletterar dataskyddsförordningens krav. Förteckningen finns på Datainspektionens hemsida (länk).

Förteckningen är dock inte uttömmande och kan komma att uppdateras och kompletteras med fler exempel framöver. Förteckningen gäller oavsett om det är fråga om personuppgiftsbehandling enbart i Sverige eller behandling av personuppgifter som är att anse som gränsöverskridande enligt definitionen i dataskyddsförordningen, artikel 4.23.

1.2. När ska konsekvensbedömningen göras?

En konsekvensbedömningen ska som huvudregel utföras innan en behandling påbörjas, men kan aktualiseras

- om risken med en pågående behandling ändras eller
- för pågående behandlingar om det inte har gjorts tidigare.

1.3. Vad ska en konsekvensbedömning innehålla?

Det finns fyra grundläggande krav i dataskyddsförordningen på vad en konsekvensbedömning ska innehålla.

1. En systematisk beskrivning av den planerade behandlingen och behandlingens syfte.

2. En bedömning av om behandlingen är nödvändig och proportionerlig i förhållande till syftet med den.
3. En bedömning av riskerna för de registrerades rättigheter och friheter.
4. De åtgärder som planeras för att hantera riskerna och för att visa att dataskyddsförordningen efterlevs.

Därutöver bör en sammantagen bedömning redovisas i konsekvensbedömningen, bl.a. om hög risk för enskildas fri och rättigheter kvarstår eller inte efter att kompensatoriska åtgärder planeras.

Dessutom ska man dokumentera att man

- rådgjort med dataskyddsombudet (om sådan finns) och
- inhämtat synpunkter från de registrerade eller deras företrädare när det är lämpligt.

För mer information, se Datainspektionens hemsida.

1.4. Börja med en riskutvärdering

I tabellen nedan listas ett antal kriterier baserade på artikel 35 i GDPR för att bedöma huruvida en konsekvensbedömning ska genomföras av en viss molntjänst. Sannolikheten för att behandlingen medför en hög risk för de registrerades fri- och rättigheter ökar ju fler kriterier som är uppfyllda i tabellen.

Kriterier	Ja	Nej
Personuppgiftsbehandlingen innefattar utvärdering eller poängtilldelning, inklusive profilering och förutsägelse av beteende.	☐	☐
Personuppgiftsbehandlingen innefattar automatiserat beslutsfattande med juridisk, ekonomisk eller annan betydande effekt för den registrerade.	☐	☐
Personuppgiftsbehandlingen innefattar att systematisk övervakning används för att observera, övervaka eller kontrollera den registrerade.	☐	☐
Behandling av känsliga personuppgifter eller extra skyddsvärd information	☐	☐
Personuppgiftsbehandlingen sker i stor skala avseende antalet berörda personer i registret, volymen av data som behandlas, varaktighet för behandlingsaktiviteten och/eller den geografiska omfattningen av behandlingsaktiviteten.	☐	☐

Det förekommer uppgifter om utsatta personer i registret.	☐	☐
Personuppgiftsbehandlingen sker med hjälp av innovativ användning eller tillämpning av tekniska eller organisatoriska lösningar.	☐	☐

Enligt Datainspektionens förteckning enligt artikel 35.4 i GDPR (2019-01-16, dnr DI-2018-13200) krävs inte någon konsekvensbedömning för behandlingar som har kontrollerats av en tillsynsmyndighet eller ett dataskyddsombud i enlighet med artikel 20 i direktiv 95/46/EG och vars genomförande inte har ändrats sedan föregående kontroll. Eftersom behandlingen är en ny är dessa undantag inte tillämpliga i aktuellt fall.

I Datainspektionens förteckning över ”när en konsekvensbedömning ska göras” räknas ett flertal omständigheter upp. Enligt anvisningarna ska en konsekvensbedömning genomföras om minst **två omständigheter** i förteckningen är uppfyllda. Bland oomständigheterna som räknas upp nämns

4. behandlar känsliga personuppgifter enligt artikel 9.2 eller uppgifter som är av mycket personlig karaktär, till exempel ett sjukhus som lagrar patientjournaler
5. behandlar personuppgifter i stor omfattning
7. behandlar personuppgifter om personer som av något skäl befinner sig i ett underläge eller i beroendeställning och därför är sårbara, till exempel barn, anställda, asylsökande, äldre och patienter

Molntjänster som uppfyller dessa omständigheter ska underkastas en dataskyddskonsekvensbedömning.

Trots att en behandling kan uppfylla två eller flera av ovanstående kriterier, kan den personuppgiftsansvarige ändå göra bedömningen att den ”sannolikt inte leder till en hög risk”. I sådana situationer bör enligt Datainspektionen den personuppgiftsansvarige motivera och dokumentera anledningarna till att en konsekvensbedömning inte utförs och inkludera dataskyddsombudets synpunkter (se Datainspektionens förteckning enligt artikel 35.4 i GDPR).

2. Rekommendationer

2.1. Tillämpliga författningar

Författningsenliga krav på sekretess, tystnadsplikt och dataskydd i socialtjänsten finns i huvudsak i följande författningar:

- Socialtjänstlagen, 2001:43 (SoL)
- Lag (1993:387) om stöd och service till vissa funktionshindrade (LSS)
- Dataskyddsförordningen (GDPR)
- Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen)
- Förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning
- Lag (2001:454) om behandling av personuppgifter inom socialtjänsten (SoLPUL)
- Förordning (2001:637) om behandling av personuppgifter inom socialtjänsten (SoLPULF)
- Offentlighets- och sekretesslagen (2019:400)

TIPS!

Det kan också vara av värde att beakta Socialstyrelsen föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården vid en riskutvärdering eller konsekvensbedömning.

Även om föreskrifterna enbart riktar sig till vårdgivare, kan viss vägledning med hänsyn till att socialtjänsten också arbetar med känsliga eller integritetskänsliga personuppgifter hämtas från dessa. I Socialstyrelsens rapport, Säker personuppgiftsbehandling i socialtjänsten - Rättsläge och utgångspunkter (2019), uppger Socialstyrelsen att det är rimligt att säkerhetsåtgärder som vidtas inom socialtjänsten sker på en nivå som motsvarar vad som gäller för personuppgiftsbehandling inom hälso- och sjukvården.

2.2. Individens användning av molntjänster

I molntjänster, bl.a. för användning vid självskattning via formulär eller enkäter, bör följande iakttas:

- Individens inloggning till molntjänsten bör ske med s.k. **stark autentisering**, dvs. med minst två faktorer som kan identifiera brukaren. BankID är en lämplig och spridd form av stark autentisering. Även engångslösenord via sms uppfyller kravet på stark autentisering. Autentisering som bygger på enbart användarnamn och ett statiskt lösenord (enfaktorsautentisering) rekommenderas inte. Det beror på att sådan autentisering har en fundamental svaghet; alla som har kännedom

om, kan räkna ut eller gissa sig till användarnamnet och lösenordet kan bli verifierade som den registrerade (behöriga) användaren i elektronisk bemärkelse. Det finns inga praktiska möjligheter för varken den enskilde eller den personuppgiftsansvarige att upptäcka att lösenordet kommit någon annan till kännedom, om inte denne avslöjar det på något sätt. Jfr. Socialstyrelsens krav på att patienter som tar del av sina elektroniska uppgifter hos en vårdgivare genom direktåtkomst ska autentiseras med två faktorer (HSLF-FS 2016:40, 4 kap. 11 §).

TIPS!

Molntjänster kan sakna stöd för BankID eller engångslösenord via sms, och det är inte självklart att barn och ungdomar som ska använda tjänsten har BankID eller mobiltelefon. Genom att stänga ned funktionen för individens självskattningshistorik (motsvarande) kan enfaktorsautentisering användas av individen vid inloggning över internet till molntjänsten. Det kräver att individen tilldelas av socialtjänsten ett alternativt ID som används som användarnamn samt ett lösenord. Individen får inte logga in med sitt namn eller personnummer. Genom att stänga av alla former av historik i molntjänsten finns därmed ingen åtkomst till personuppgifter, givet att en påbörjad enkät som avbryts av invånaren raderas på servern.

- Överföringen av personuppgifter från individens dator eller en app i en mobil enhet till molntjänsten bör ske via en krypterad förbindelse i öppna nät, t.ex. internet. Inga uppgifter bör sparas på individens dator eller mobila enhet efter överföring.

TIPS!

Tänk på att vissa individer saknar internetåtkomst, dator eller mobil. Kontrollera om leverantören/tjänsten kan stödja individer i sådana situationer genom att de får låna en mobil enhet av socialtjänsten med en lokalt installerad instans av applikation. Registrering av uppgifter sker då off-line. Den mobila enheten bör konfigureras så att individen kan spara enkäter eller formulär i den mobila enheten. Åtkomst sker med användar-ID och lösenord. Enbart socialtjänsten (inte leverantören) har spårbarhet på användarna i tjänsten.

Det erinras att det alltjämt är ”personuppgifter” i dataskyddsförordningens mening, men pseudonymiserade. Applikationen ska låsa sig själv inom vissa minuter vid inaktivitet och bevara registrerade uppgifter krypterat. Ansvarig handläggare hämtar den mobila enheten efter viss tid vid hembesök och kan ladda upp innehållet i molntjänsten på arbetsplatsen. När uppgifter överförs till tjänsten ska all data i den mobila enheten raderas.

2.3. Fritextfält

Fritextfält i molntjänster bör undvikas. Det finns en påtaglig risk för registrering av andra fysiska personer vid namn samt känsliga personuppgifter om individen själv. Leverantörens servrar riskerar att lagra personuppgifter om fysiska personer vid namn och kräver manuellt arbete för att ”rensas” bort. Det finns vidare en risk att aggregering av data blir ett mödosamt arbete eftersom namn på fysiska personer måste tas bort manuellt, med risk att uppgifter exponeras ändå.

Om möjligt ta bort fritextfält i molntjänsten, t.ex. i formulär. Använd ja/nej-frågor eller alternativa svar med kryssrutor. Om fritextfält anses som nödvändiga, begränsa antalet tecken till en lämplig nivå.

TIPS!

En positiv effekt av att det inte finns fritextfält är att socialtjänstens personal kan bli mer motiverade att uppsöka individen för samtal om insatsen.

2.4. Personalens åtkomst till molntjänsten

Beträffande personal inom socialtjänsten och deras åtkomst till individers personuppgifter i molntjänster finns det skäl att hänvisa till Socialstyrelsens rapport, *Säker personuppgiftsbehandling i socialtjänsten - Rättsläge och utgångspunkter* (2019). I rapporten uppger Socialstyrelsen att det är rimligt att säkerhetsåtgärder som vidtas inom socialtjänsten sker på en nivå som motsvarar vad som gäller för personuppgiftsbehandling inom hälso- och sjukvården.

Av Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården framgår att hälso- och sjukvårdspersonal som loggar in på tjänster över öppna nät, t.ex. internet, ska autentisera sig med en stark autentisering (3 kap. 15 §). Det är rimligt att socialtjänsten iakttar samma krav. Exempel på lösningar för stark autentisering är BankID, engångslösenord via sms eller SITHS-kort.

2.5. Vilken information ska hanteras i molntjänsten?

Ett första steg är att göra en kartläggning. Genom en kartläggning kan verksamheten få en uppfattning om vilka typer av uppgifter som kan komma att hanteras i molntjänsten. Med denna kunskap kan man bedöma hur skyddsvärd informationen är ur ett individ-, verksamhets- och samhällsperspektiv, och om det över huvud taget är lämpligt att hantera informationen i en molntjänst.

Nästa steg är att ta ställning till vilka rättsregler som är tillämpliga i t.ex. offentlighets- och sekretesslagen, dataskyddsförordningen eller särskild registerförfattning. Vilka legala krav på sekretess eller tystnadsplikt som ställs när uppgifter från verksamheten ska hanteras i en molntjänst beror bland annat på vilken typ av information det rör sig om. Alla myndigheter som anlitar en molntjänstleverantör för att bearbeta, lagra eller på annat sätt hantera kommunens eller regionens information måste bedöma 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.

TIPS!

I kartläggningsarbetet ingår bl.a. informationsklassning och riskanalys, se informationssäkerhet kap 2.7 respektive dataskyddskonsekvensbedömning kapitel 1.

2.6. Utländska molntjänstleverantörer

Om verksamheten överväger att använda en utländsk molntjänst (varmed menas att leverantören har sitt säte i ett annat land eller har upprättat sina datacenter i annat land) måste särskilda överväganden göras. Dataskyddsförordningen lägger normalt sett inga hinder för att anlita leverantörer med hemvist och ursprung inom EU. Om molntjänsten hanterar sekretessbelagda personuppgifter bör kontroll utföras att lagstiftningen i leverantörens hemland ålägger dennes medarbetare en straffsanktionerad tystnadsplikt som kan jämställas med brott mot tystnadsplikt som finns i den svenska brottsbalken (böter eller fängelse i upp till ett år).

Om leverantören har sin hemvist i ett land utanför EU/EES-området, eller datacenters ligger i ett sådant s.k. tredje land, krävs att vissa förutsättningar i dataskyddsförordningen är uppfyllda. Precis som för uppgifter som omfattas av sekretess bygger regelverket på att verksamheten 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.

Man bör särskilt undersöka om molntjänsteleverantör utanför EU/EES har antagit EU-kommissionens standardavtalsklausuler eller att företagskoncernen har antagit bindande företagsbestämmelser, s.k. Binding Corporate Rules, (BCR), som beslutas av ansvarig dataskyddsmyndighet på ansökan av koncernen.

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

2.7. Informationssäkerhet

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 mot leverantör och molntjänsten. 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.

Ett lämpligt tillvägagångssätt är att samla berörda medarbetare till en workshop om informationssäkerheten. Under en workshop diskuteras olika risker och tänkbara hot, vad det innebär om obehöriga kommer åt informationen och så vidare. Allting dokumenteras för att sedan användas i olika kravställningar, för intern information och till viss del extern. Det här kallas informationssäkerhetsklassificering respektive risk- och sårbarhetsanalys och innebär i stora drag att verksamheten beslutar vilket värde informationen i molntjänsten har. Utöver, eller snarare som en del av det arbetet ska också en bedömning utifrån dataskyddslagstiftningen och en konsekvensbedömning göras och dokumenteras. SKR har tagit fram mallar att använda för dokumentation i det arbetet (länk).

TIPS!

Deltagare på workshopen bör vara:

- Systemförvaltare
- Informationsägare (någon som på relativt hög nivå kan besluta om vägval och avgränsningar)
- Användare av systemet (med digital kompetens och från olika delar av verksamheten)
- It-arkitekt
- Informationssäkerhetsansvarig
- Jurist eller dataskyddsombud

Under mötet, som leds av informationssäkerhetsansvarig tillsammans med projektledaren, går man igenom vilken information som kommer att finnas i systemet. Även vilka lagrum man har att förhålla sig till och hur viktigt det är för verksamheten att informationen kan garanteras utifrån dessa perspektiv:

- Riktighet – vikten av tillförlitlig, korrekt, fullständig information
- Konfidentialitet– vikten av åtkomstbegränsning, insynsskydd
- Spårbarhet – vikten av att kunna spåra olika händelser i systemen
- Tillgänglighet– vikten av tillgång till informationen inom önskad tid

Det handlar alltså om att genom informationssäkerhetsklassificeringen avgöra vilken nivå av säkerhet informationen behöver ha. Det finns fyra nivåer, där nivå 1 innebär ringa skada för verksamheten om det finns brister i till exempel informationens riktighet. Om man bedömer att verksamheten skulle drabbas av allvarlig eller katastrofal skada vid brister i informationen blir klassningen Nivå 4.

Varje kategori, riktighet, konfidentialitet, spårbarhet och tillgänglighet, bedöms separat. Klassificeringen resulterar i olika krav på molntjänsten när det gäller inloggning och behörighetsstyrning med mera.

Nästa steg i arbetet med informationssäkerhet är att göra en risk- och sårbarhetsanalys.

Utifrån informationsklassningen fortsätter man diskussionen kring vilka eventuella hot och risker man ser, hur sannolikt det är att de inträffar och vilken konsekvens det skulle kunna få för verksamheten.

När arbetet med informationsklassning och risk- och sårbarhetsanalys är klart omsätts det till ett antal krav så att informationen i tjänsten skyddas på det sätt som behövs. Det kan vara åtgärder som behövs internt eller av leverantören. Det kan röra allt från interna processer som behöver ses över till interna avtal mellan verksamhet och it.

TIPS!

En intern process som är viktig är kontinuitetsplaner för att så bra som möjligt kunna hantera situationer där molntjänsten är otillgängliga under såväl kort som lång sikt.

För att förenkla informationsklassning av molntjänster samt förbättra stöd för löpande systemförvaltning och kravställning vid upphandling, har SKR tagit fram webbverktyget KLASSA, (länk). Via KLASSA kan verksamheten få ut handlingsplaner avseende informationssäkerhetsarbete för molntjänsten, men också konkreta krav inför eventuell upphandling av molntjänsten.

2.8. Avtal och dokumentation

En grundregel för alla avtal är att det ska råda balans mellan beställare och leverantör, mellan åtaganden och skyldigheter.

Har man gjort en informationssäkerhetsklassning är verksamhetens krav på hur informationen i tjänsten ska hanteras tydliggjorda. Kraven ska i sin tur återspeglas i avtalen. När det gäller molntjänster är delarna kring dataöverföring extra viktiga att ha koll på.

Avtal för molntjänster består i princip av följande:

- Huvudavtal - där de kommersiella villkoren regleras
- Personuppgiftsbiträdesavtal - där rättigheter och skyldigheter för främst leverantören regleras inklusive instruktioner till densamme för hanteringen av personuppgifter. SKR-koncernen har tagit fram ett personuppgiftsbiträdesavtal (PUB-avtal) för regioner och kommuner som bör användas (länk).
- EU-kommissionens standardavtalsvillkor för leverantörer i tredje land (klausuler anpassade för gränsöverskridande personuppgiftsöverföring; kan ersätta personuppgiftsbiträdesavtal). Alternativt att om leverantören är ett amerikanskt bolag är ackrediterad enligt Privacy Shield.

Privacy Shield är en överenskommelse om skydd för personuppgifter mellan EU och USA och leverantörer behöver certifiera sig och anmäla att de följer de principer regelverket innehåller.

TIPS!

Det kan kännas osäkert med webbavtal där man klickar i ”I accept” som signering. Spara därför ner avtalen med datumstämpel och komplettera med en skärmbild på acceptansrutan. Finns det frågor om innehållet i avtalen – kontakta leverantören.

Det är bra att ta fram olika underlag inför användandet av molntjänster för att förtydliga för olika målgrupper varför och hur tjänsten ska användas, vem som ansvarar för olika delar och så vidare. Några exempel på dokument som kan vara bra att ha är följande:

- Kommunikationsplan för processen för att ta i anspråk en molntjänst
- Rutiner och roller för användningen av tjänsten (vem som ansvarar för vad, tidsperiod, kontohantering etc.)
- Informationsspecifikation (tjänstespecifik beskrivning av tjänsten)
- Manualer av olika slag och för olika roller.

3. Konsekvenser vid en Brexit

Storbritannien ska lämna den Europeiska unionen och betraktas därmed som ett s.k. tredje land enligt dataskyddsförordningen. Det får vissa konsekvenser för en socialnämnd (motsvarande) som använder eller avser att upphandla en molntjänst från en brittisk leverantör.

Enligt tillgänglig information i skrivande stund kommer enligt överenskommelse mellan Storbritannien och EU en övergångsperiod att löpa till 31 december 2020, under vilken tid gällande EU-regler kommer att fortsätta att gälla för Storbritannien och förhandlingar om nästa steg kan inledas.

Under den övergångsperioden gäller alltjämt dataskyddsförordningen i Storbritannien. Personuppgifter kan överföras fritt mellan Storbritannien och EU, och brittiska företag ska beakta regelverket. Under denna övergångsperiod kommer den brittiska regeringen och EU att förhandla om ett dataskyddsarrangemang som passar båda parter, oavsett om det är ett beslut av Kommissionen om att Storbritannien anses ha ett adekvat skydd eller ett avtal mellan EU och landet som garanterar skyddet av personuppgifter och som gör att personuppgifter kan röra sig fritt mellan Storbritannien och EU. Storbritannien och EU har sagt att de är enade om att säkerställa en hög nivå av

skydd av personuppgifter för att underlätta datautbyte mellan dem och hoppas ha träffat avtal i slutet av övergångsperioden.

Det är svårt att bedöma i nuläget vilket arrangemang som parterna slutligen bedömer som lämpligast. Ett beslut av Kommissionen om att personuppgifter har ett adekvat skydd i Storbritannien i enlighet med dataskyddsförordningens standarder är det mest troliga och önskvärda resultat eftersom landet anpassat sin nationella lagstiftning till förordningen och föredömligt efterlevt den. I sådant fall krävs inga särskilda åtgärder från en kommuns sida utöver att teckna personuppgiftsbiträdesavtal (PUB-avtal), varvid SKR-koncernens mallar för PUB-avtal med fördel kan användas och som även finns översatt till engelska. Länk till avtal finns under kapitel 2.8. Avtal och dokumentation. Ett annat scenario är att Kommissionens standardavtalsklausuler måste användas (se ovan).