Sveriges Kommuner och Regioner

PROMEMORIA

2025-05-28

Olof Widgren, avdelningen för juridik

Kan Mina meddelanden användas för att skicka information som omfattas av sekretess?

Sammanfattning

Mina meddelanden är en teknisk infrastruktur för digital post där leverantörerna av vidareförmedlingstjänster (vidareförmedlaren) inom infrastrukturen i allmänhet bedriver endast teknisk bearbetning och teknisk lagring i OSL:s mening. Detta rekvisit i den sekretessbrytande bestämmelsen i 10 kap 2 a § OSL är därför *typiskt sett* uppfyllt i förhållande till sådana leverantörer, men en individuell bedömning behöver ändå göras i det enskilda fallet för att säkerställa att vidareförmedlarens aktiviteter faller inom begreppet endast teknisk bearbetning och teknisk lagring.

Om det framkommer att vidareförmedlaren använder informationen för andra ändamål än att endast tekniskt bearbeta och tekniskt lagra informationen åt utlämnande myndighet är dock bestämmelsen inte tillämplig i förhållande till den hanteringen.

I de fall vidareförmedlaren ägnar sig åt endast teknisk bearbetning och teknisk lagring, ska det även göras en bedömning av om det är olämpligt att lämna ut informationen till leverantörerna inom infrastrukturen. I de flesta fall bör det inte ses som olämpligt att göra detta, även om en bedömning behöver göras i förhållande till den enskilda vidareförmedlingstjänsten och den typ av information som ska skickas. När det gäller viss specifik information av särskilt känsligt slag, t.ex. uppgifter som rör totalförsvaret eller som är säkerhetsskyddsklassificerad enligt säkerhetsskyddslagen kan det dock vara olämpligt att skicka informationen via Mina meddelanden, i den mån det blir aktuellt.

Sveriges Kommuner och Regioner
info@skr.se, www.skr.se
Post: 118 82 Stockholm *Besök:* Hornsgatan 20
Tfn: 08-452 70 00 *Org nr:* 222000-0315

Bakgrund

Inom SKR-koncernens strategiska agenda Handslag för digitalisering genom välfärdsutveckling (Handslaget) är ett av initiativen ett införandestöd för digital post. Initiativet syftar bl.a. till att öka medlemmarnas användning av digital post, genom att nyttja den tekniska infrastrukturen Mina meddelanden som förvaltas av Myndigheten för digital förvaltning (Digg). Under arbetet har frågan väckts om även sekretessbelagd information kan skickas via s.k. vidareförmedlingstjänster som många medlemmar som använder Mina meddelanden anlitar. Denna promemoria syftar till att belysa denna frågeställning. Promemorian har tagits fram inom Kompetensgemenskapen för digitaliseringsjuridik, en arbetsgrupp med representanter från SKR, Adda, Inera och ett antal kommuner som bildats inom Handslaget. Promemorian är framtagen av tjänstepersoner och är inte formellt beslutade av de enskilda huvudmän som dessa tjänstepersoner representerar.

Bestämmelsen i 10 kap. 2 a § OSL

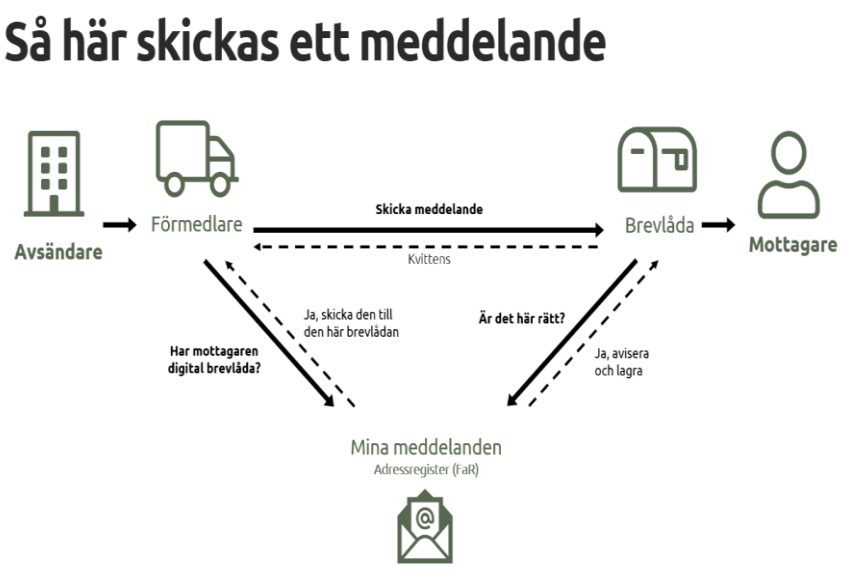
I juli 2023 infördes en ny sekretessbrytande bestämmelse i i offentlighets- och sekretesslagen (OSL), 10 kap 2 a §. Bestämmelsen har följande lydelse. *Sekretess hindrar inte att en uppgift lämnas till en enskild eller till en annan myndighet som för den utlämnande myndighetens räkning har i uppdrag att endast tekniskt bearbeta eller tekniskt lagra uppgiften, om det med hänsyn till omständigheterna inte är olämpligt att uppgiften lämnas ut*.

Av förarbetena till bestämmelsen framgår att uppgifter som lagras eller på annat sätt hanteras av en extern leverantör av IT-tjänster anses röjda i OSL:s mening, vilket tidigare varit omdiskuterat (prop. 2022/23:97, s. 7 se även eSams Vägledning Utkontraktering – sekretess och dataskydd ES2023-06, s. 24, nedan ”eSams vägledning”). I och med det ställningstagandet ansågs det finnas behov av en sekretessbrytande bestämmelse för att myndigheter ska kunna anlita externa aktörer för t.ex. IT-drift (se vidare anf. prop. s. 9 ff).

Bestämmelsens tillämpning i förhållande till digitala utskickstjänster/vidareförmedlare inom IT-infrastrukturen Mina meddelanden

När meddelanden ska skickas inom Diggs infrastruktur för digital post (Mina meddelanden) används ofta en vidareförmedlare/utskickstjänst, som tillhandahålls av en extern leverantör. I skissen nedan kallas leverantören för förmedlare (nedan i löptexten även benämnd vidareförmedlare).

Sveriges Kommuner och Regioner
info@skr.se, www.skr.se
Post: 118 82 Stockholm *Besök:* Hornsgatan 20
Tfn: 08-452 70 00 *Org nr:* 222000-0315



I och med att leverantören av denna tjänst kommer att ha tillgång till den information som skickas kommer eventuella uppgifter som omfattas av sekretess att anses röjda för leverantören. Detta gäller i och för sig inte om uppgifterna skyddas av en kryptografisk funktion som hindrar mottagaren att ta del av uppgiftens informationsbärande innehåll, (se prop. 2022/23:97, s. 7), men den situationen bedöms sällan bli aktuell i kommunal verksamhet. Utgångspunkten vid anlitande av en extern vidareförmedlare är således att uppgifterna som leverantören hanterar anses röjda i OSL:s mening. De frågeställningar som kommer att redogöras för i det följande rör alltså situationen att utskick av digital post utkontrakterats genom anlitande av en leverantör av en vidareförmedlingstjänst.

Ett sådant röjande är tillåtet om sekretess inte hindrar att uppgiften lämnas ut. Så är t.ex. fallet när det finns en sekretessbrytande bestämmelse som är tillämplig. Mot bakgrund av den stora mängd information som kan antas skickas via Mina meddelanden och att dessa i varierande grad innehåller uppgifter som omfattas av sekretess av olika styrka och räckvidd, är det i praktiken omöjligt att bedöma utlämnandet av varje uppgift för sig, vilket annars normalt sett sker vid prövning av om en handling kan lämnas ut helt eller delvis. I den mån Mina meddelanden kommer att användas för att skicka information som innehåller sekretessbelagda uppgifter via en extern leverantör av förmedlingstjänster kommer förfarandet vara beroende av att utlämnande kan ske med stöd av den sekretessbrytande bestämmelsen i 10 kap 2 a § OSL. Bestämmelsens tillämplighet beror i sin tur på två rekvisit, dels om leverantörens befattning med uppgifterna utgör endast teknisk bearbetning och teknisk lagring för myndighetens räkning, och, om så är fallet, att det inte är olämpligt att lämna ut uppgifterna. Dessa förutsättningar diskuteras nedan.

Innebörden av begreppet endast teknisk bearbetning och teknisk lagring

Av förarbetena till 10 kap 2 a OSL framgår bl.a. följande.

Innebörden av uttrycket teknisk bearbetning eller teknisk lagring är densamma som i 2 kap. 13 § första stycket tryckfrihetsförordningen (jfr 2 kap. 9 § tredje stycket tryckfrihetsförordningen). Ett uppdrag att tekniskt bearbeta eller tekniskt lagra uppgifter kan exempelvis bestå i att införa, förvalta, utveckla och så småningom avveckla en it-driftstjänst. Under dessa olika faser kan en mängd olika åtgärder behöva vidtas för att upprätthålla den tillgänglighet, funktionalitet och prestanda i tjänsten som har avtalats mellan parterna. Det kan röra sig om förändring och tillägg i en befintlig tjänsts funktionalitet, etablering av en tilläggstjänst, integration med andra tjänster, konfiguration, test och utveckling samt tillhandahållande av supporttjänster. Det kan också röra sig om säkerhetstester och andra säkerhetshöjande åtgärder som uppgradering, uppdatering, säkerhetskopiering, kryptering, anonymisering, pseudonymisering och incidenthantering. Vid avveckling av en tjänst kan myndighetens uppgifter behöva migreras eller exporteras tillbaka till myndigheten eller till en annan uppdragstagare. Vilka slags åtgärder som kan omfattas av uttrycket teknisk bearbetning eller teknisk lagring kan komma att förändras över tid med anledning av den tekniska utvecklingen. Att det ska vara fråga om endast teknisk bearbetning eller teknisk lagring hindrar inte att personal hos uppdragstagaren tar del av de uppgifter som hanteras för den uppdragsgivande myndighetens räkning. Det kan vara nödvändigt för att personalen ska kunna utföra sina arbetsuppgifter som ett led i den tekniska bearbetningen eller tekniska lagringen. Främst handlar det om drifts- och säkerhetsrelaterad information, exempelvis uppgifter om användarkonton, loggar, krypteringsnycklar, lösenord och säkerhetsinställningar. Det kan dock också röra sig om andra uppgifter i läsbar form.

I förarbetena till lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter (tystnadspliktslagen) har liknande uttalanden gjorts om innebörden av begreppet endast teknisk bearbetning och teknisk lagring. Där uttalas bl.a. följande (s. 22-23).

Innebörden av teknisk bearbetning eller teknisk lagring är densamma som i 2 kap. 9 § tredje stycket tryckfrihetsförordningen (jfr 2 kap. 13 § första stycket tryckfrihetsförordningen). Vilka slag av åtgärder som kan omfattas av teknisk bearbetning eller teknisk lagring behöver tolkas i förhållande till dagens digitala informationshantering och den fortgående tekniska utvecklingen. En tjänsteleverantör kan exempelvis ha i uppdrag att införa, förvalta, utveckla och så småningom avveckla en tjänst åt en myndighet. Tjänsteleverantören kan under dessa olika faser behöva vidta en mängd olika åtgärder som innefattar teknisk bearbetning eller teknisk lagring av uppgifter för att upprätthålla den tillgänglighet, funktionalitet och prestanda i tjänsten som har avtalats mellan parterna. Sådana åtgärder kan röra sig om förändring och tillägg i en befintlig tjänsts funktionalitet, etablering av en tilläggstjänst, integration mot andra tjänster, konfiguration, test och utveckling samt tillhandahållande av supporttjänster. Det kan också röra sig om säkerhetshöjande åtgärder som uppgradering, uppdatering, säkerhetskopiering, kryptering, anonymisering, pseudonymisering och incidenthantering. Vid avveckling av en tjänst kan myndighetens information behöva migreras eller

exporteras tillbaka till myndigheten eller till en annan tjänsteleverantör. Under samtliga moment av teknisk bearbetning eller teknisk lagring kan det förekomma att personal hos tjänsteleverantören tar del av de uppgifter som hanteras för den uppdragsgivande myndighetens räkning. Detta kan vara nödvändigt för att de ska kunna utföra sina arbetsuppgifter som ett led i den tekniska bearbetningen eller tekniska lagringen. Det torde normalt röra sig om drifts- och säkerhetsrelaterad information, t.ex. uppgifter om användarkonton, loggar, krypteringsnycklar, lösenord och säkerhetsinställningar. Men det kan också röra sig om uppgifter i läsbar form (jfr prop. 1975/76:160 s. 87).

Esam har uttalat bl.a. följande om bestämmelsen.

10 kap 2 a § OSL syftar till att ge förutsättningar för myndigheter att utkontraktera sin IT-drift (prop. 2022/23:97. s. 1 och 10 och eSams vägledning s. 26). I förarbetena till bestämmelsen anges diarie- och ärendehanteringssystem, system för kontorsstöd vilket kan inkludera e-post, kalender och dokumenthanteringsstöd som exempel på IT-drift som kan bli föremål för utkontraktering. Det anges inte specifikt att de angivna exemplen är att betrakta som exempel på teknisk bearbetning eller teknisk lagring. Avsikten med att ange dessa exempel får dock antas ha varit att peka på möjliga tjänster för teknisk bearbetning eller teknisk lagring. Härutöver beskrivs endast översiktligt att de grundläggande it-driftstjänster som myndigheter har behov av kan utgöra teknisk bearbetning eller teknisk lagring (eSams vägledning s. 13).

Enligt eSams uppfattning ska en tjänsteleverantörs förhållningssätt och befattning med informationsmängden i en utkontraktering alltså vara av teknisk natur och uteslutande för den utkontrakterande myndighetens räkning. Någon behandling av tjänsteleverantören för egen räkning kan inte tillåtas. Om tjänsteleverantörens befattning med uppgifterna är av teknisk natur är det acceptabelt att denne tar del av nödvändiga uppgifter i klartext, dvs. eSam gör bedömningen att förarbetsuttalandena till tystnadspliktslagen och 10 kap. 2 a § OSL och även tidigare förarbetsuttalanden till TF ger ett vidare utrymme att “ta del” av uppgifter än vad tidigare praxis uttryckt. eSam anser således att för att det ska vara fråga om teknisk bearbetning eller teknisk lagring ska informationsbehandlingen ske för den utkontrakterade myndighetens räkning och behandlingen får inte innebära att informationen förädlas genom att något tillförs innehållsmässigt. I rekvisitet “endast” ligger att uppgifterna inte får hanteras på annat sätt än för teknisk bearbetning eller teknisk lagring. Om samma uppgifter hanteras i ett annat informationsflöde behöver dessa flöden enligt eSams uppfattning hållas åtskilda, annars riskerar hela utkontrakteringen att inte anses vara teknisk bearbetning eller teknisk lagring. Myndigheten behöver därmed säkerställa en åtskild hantering av leverantören, i de fall leverantören också tillhandahåller andra tjänster där uppgifterna hanteras. Detta behöver hanteras särskilt i avtalsregleringarna och tekniska begränsningar såsom behörighetsbegränsningar (eSams vägledning s. 18-19).

Diskussion om innebörden av begreppet ”endast teknisk bearbetning och teknisk lagring”

Det är vanligt att leverantörer av IT-tjänster hanterar information som omfattas av sekretess. Mot denna bakgrund bör begreppet ”endast teknisk bearbetning och teknisk lagring” ges en relativt vidsträckt innebörd. Vad som uttalas i förarbetena till bestämmelsen ger också i viss mån stöd för att begreppet ska tolkas extensivt. Ett exempel på det är att det uttryckligen

sägs att begreppet inte hindrar att leverantören tar del av uppgifter i läsbar form. Vidare skulle en snäv tolkning av begreppet göra att samarbete med privata tjänsteleverantörer allvarligt försvåras eller t.o.m. omöjliggörs, eftersom sådant samarbete inom offentlig verksamhet regelmässigt kommer innebära att uppgifter som omfattas av sekretess röjs för tjänsteleverantören. Sådana konsekvenser av bestämmelsen kan inte rimligen ha varit avsedda, särskilt som det uttalade syftet med bestämmelsen varit att ge förutsättningar för myndigheter att utkontraktera sin IT-drift (prop. 2022/23:97 s. 1 och 10).

Exakt vilka tjänster eller åtgärder som en tjänsteleverantör kan utföra inom ramen för begreppet teknisk bearbetning eller teknisk lagring är inte en gång för alla bestämt och kommer inte heller framgent att kunna utläsas direkt från lagtext eller andra rättskällor. Detta mot bakgrund av dels hur lagstiftningen är konstruerad där en bedömning ska göras i förhållande till enskilda leverantörer, dels den tekniska utvecklingen som kan förväntas leda till en ökning av att både antalet och typen av tjänster som leverantörer kan erbjuda.

Med stöd av bl.a. förarbetena till 10 kap 2 a § OSL är det dock rimligt att utgå ifrån att verksamheten hos en digital utskickstjänst inom ramen för den infrastrukturen Mina meddelanden *typiskt sett* innebär just sådan teknisk bearbetning och teknisk lagring som avses i bestämmelsen. I annat fall skulle tjänsten och andra liknande tjänster i många fall bara kunna tillämpas för att skicka offentlig information, d.v.s. information som inte omfattas av sekretess. Användningsområdet för Mina meddelanden och andra liknande tjänster skulle då minska avsevärt. Även detta skulle strida mot det uttryckliga ändamålen med bestämmelsen i 10 kap 2 a § att underlätta utkontraktering av IT-tjänster. Det skulle även motverka regeringens ambitioner på digitaliseringsområdet.

Utgångspunkten bör mot denna bakgrund vara att en digital utskickstjänst/vidareförmedlare inom Mina meddelanden ägnar sig åt teknisk bearbetning och lagring i OSL:s mening och att detta rekvisit in hindrar att sekretessbelagd information skickas via en sådan vidareförmedlare. En bedömning behöver dock göras i det enskilda fallet, bl.a. av att leverantören inte ges rätt att förädla informationen genom att tillföra något innehållsmässigt till den. Vidare vore det, för det fall utskickstjänsten även hanterar manuella utskick, att rekommendera att denna del avtalsmässigt hålls åtskild från den digitala hanteringen. Det finns annars risk för att manuell hantering som faller utanför begreppet ”teknisk bearbetning och teknisk lagring” gör att hela utkontrakteringen faller utanför tillämpningsområdet för 10 kap 2 a § OSL och därmed riskerar att inte kunna genomföras (se eSams vägledning s. 19).

När är det olämpligt att röja uppgifter för teknisk bearbetning och lagring?

För att 10 kap 2 a § OSL ska kunna tillämpas krävs som nämnts ovan även att det inte är olämpligt att lämna ut informationen till leverantören.

Av förarbetena (anf. prop. s. 17) framgår bl.a. följande.

Det ska vid bedömningen av om det är olämpligt att lämna ut uppgifter göras en allsidig prövning av alla omständigheter som är relevanta i det enskilda fallet. Omständigheter som kan ha betydelse är exempelvis vilken typ av uppgifter det rör sig om, vilka intressen som ligger till grund för sekretessen och uppgifternas omfattning. En omständighet som med viss tyngd kan tala emot ett utlämnande är att det är fråga om uppgifter av särskilt känsligt slag, exempelvis uppgifter av synnerlig betydelse för rikets säkerhet när det gäller totalförsvaret. Det bör också beaktas vilka åtgärder som uppgiftsmottagaren vidtar för att skydda uppgifterna och om denne omfattas av en lag- eller avtalsreglerad tystnadsplikt. Även avtalsförhållandet mellan parterna ska beaktas och då i synnerhet sådana avtalsvillkor som riskerar att frånta den utlämnande myndigheten kontrollen över uppgifterna. Var uppgifterna kommer att hanteras geografiskt kan ha betydelse liksom om det förekommer underleverantörer som potentiellt kan få tillgång till uppgifterna. Vidare ska den utlämnande myndigheten ta hänsyn till om de uppgifter som lämnas ut kommer att samlokaliseras med uppgiftsmängder som tillhör andra kunder och bedöma om detta innebär några särskilda risker. Det kan vara lämpligt att den uppgiftsutlämnande myndigheten dokumenterar de avvägningar och bedömningar som görs vid ett utlämnande som omfattar en större uppgiftsmängd eller uppgifter som är av känslig karaktär. Om det rör sig om säkerhetsskyddsklassificerade uppgifter gäller härutöver särskilda bestämmelser enligt säkerhetsskyddslagen (2018:585).

Esam har uttalat följande om detta led i bestämmelsen (eSams vägledning s. 26-27).

I och med att bestämmelsen gäller uppgifter som mottagaren erhåller för teknisk bearbetning eller teknisk lagring omfattas uppgifterna även av sekretess hos mottagaren, se 11 kap. 4 a § och 40 kap. 5 § OSL eller av tystnadsplikt enligt 4 § i lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter (tystnadspliktslagen). Tystnadsplikt enligt den senare lagen gäller enligt dess 3 § även för anställda m.fl. hos underleverantörer till tjänsteleverantören, som medverkar till att fullgöra dennes uppdrag. Lagen är begränsad till teknisk bearbetning eller lagring av uppgifter i samband med utkontraktering, varför uppdrag som innehåller annat än enbart sådana tekniska moment faller utanför lagens tillämpningsområde i dessa delar.

I förarbetena till 10 kap. 2 a § OSL anges att bestämmelsen endast kan tillämpas av de myndigheter och med myndigheter jämställda organ som omfattas av OSL:s tillämpningsområde, och att en privat tjänsteleverantör, som inte omfattas av OSL, därmed inte kan tillämpa bestämmelsen när denne avser att exempelvis överföra uppgifter till en underleverantör. Enligt eSams uppfattning innebär inte detta ett hinder mot att utkontraktera till en leverantör som använder underleverantörer. Förekomsten av underleverantörer är däremot något som måste beaktas vid myndighetens olämplighetsprövning.

Diskussion om olämplighetsbedömningen

Lagtexten och förarbetena ger endast allmänt hållen vägledning om vilka faktorer som ska beaktas vid bedömningen av om det är olämpligt att lämna ut uppgifter för endast teknisk bearbetning och teknisk lagring till en extern leverantör. Det nämns att om tystnadsplikt gäller för leverantören enligt lag eller avtal är det en omständighet som talar för att det inte är olämpligt att lämna ut uppgifterna. Bedömningen ska dock ske rörande uppgifter som lämnats ut för endast teknisk bearbetning och teknisk lagring, vilka omfattas av tystnadsplikt antingen enligt tystnadspliktslagen eller OSL. För aktörer som omfattas av dessa lagstiftningar, d.v.s. aktörer som har sitt säte i Sverige eller på annan grund faller inom svensk jurisdiktion, gäller alltså tystnadsplikt enligt lag vid denna typ av utkontraktering. För aktörer som faller utanför svensk jurisdiktion, t.ex. många aktörer med säte utomlands, gäller dock inte dessa lagstadgade tystnadsplikter. Tystnadsplikten får i dessa fall istället säkerställas genom avtal.

Mot att lämna ut uppgifterna talar enligt förarbetena att det är fråga om uppgifter av särskilt känsligt slag, t.ex. uppgifter av synnerlig betydelse för rikets säkerhet när det gäller totalförsvaret. Uttrycket ”synnerlig betydelse för rikets säkerhet” nämns endast i på två ställen i i OSL, i 5 kap 5 § och i 15 kap 5 § och avser uppgifter vars utlämnande endast får prövas av viss myndighet enligt förordning beslutad av regeringen. En bestämmelse finns vidare i 1 § offentlighets- och sekretessförordningen (2009:641) enligt vilken utlämnande till en enskild av en allmän handling som är av synnerlig betydelse för rikets säkerhet endast får prövas av chefer för vissa departement eller av statsministern.

Det förefaller dock osannolikt att det endast är uppgifter som nämns i dessa bestämmelser som lagstiftaren anser vara olämpliga att lämna ut för endast teknisk bearbetning och teknisk lagring, särskilt mot bakgrund av att förarbetsuttalandet inte bara tar sikte på rikets säkerhet utan även på totalförsvaret. Att totalförsvaret nämns väcker frågan om även uppgifter som omfattas av 15 kap 2 § OSL kan vara olämpliga att lämna ut för teknisk bearbetning och teknisk lagring. Detta kan dock inte gälla utan undantag eftersom många offentliga aktörer hanterar information som faller under 15 kap 2 § OSL. Förarbetena talar även för att hänsyn bör tas till om informationen är säkerhetsskyddsklassificerad enligt säkerhetsskyddslagen (1 kap. 2 § andra stycket). För sådan information gäller särskilda krav enligt säkerhetsskyddslagen och säkerhetsskyddsförordningen och sådan information bör mot denna bakgrund som utgångspunkt inte hanteras i Mina meddelanden. Under alla omständigheter bör det vara fråga om väldigt känslig information för att det ska anses olämpligt att lämna ut den för endast teknisk bearbetning och teknisk lagring. Vidare lär det vara relativt ovanligt att det blir aktuellt för kommuner och regioner att skicka

sådan information via Mina meddelanden, bl.a. eftersom mottagarna av försändelserna som skickas via denna kanal är privatpersoner och företag, som normalt inte har behov av att ta del av sådan information.

Även förekomsten av underleverantörer behöver beaktas vid bedömning av om det är olämpligt att lämna ut informationen till en vidareförmedlare. I den mån det finns personuppgiftsbiträdesavtal mellan ansvarig kommun och en huvudleverantör av en sådan tjänst är det lämpligt att genom detta avtal ställa krav på att huvudleverantören endast anlitar underleverantörer/underbiträden som lever upp till motsvarande krav på säkerhet som huvudleverantören själv åtagit sig att uppfylla i personuppgiftsbiträdesavtalet.[1]

Vidare kan liknande krav som de som ställs i ett personuppgiftsbiträdesavtal om att en leverantör ska uppfylla vissa säkerhetskrav vara lämpliga att ställa på vidareförmedlare som ska hantera sekretessbelagd information, även i den fall där vidareförmedelaren inte ses som personuppgiftsbiträde och det således inte tecknas något personuppgiftsbiträdesavtal. Säkerhetskraven får då regleras i tjänsteavtalet/huvudavtalet.

Särskilt om systematiskt informationssäkerhetarbete inför utkontraktering

Ett sätt att hantera olämplighetsbedömningen enligt 10 kap 2 a § OSL är att koppla samman den med det generella systematiska informationssäkerhetsarbete som bedrivs inom en organisation och som bl.a. kan aktualiseras vid en utkontraktering. Inför en utkontraktering är det t.ex. ofta värdefullt att göra analyser rörande informationssäkerhet och dataskydd. Genom en informationskartläggning identifieras vilken information/typ av uppgifter som omfattas av utkontrakteringen. Genom informationsklassning bestäms informationens skyddsvärde och genom denna kan det gå att identifiera vilken eventuell sekretessbestämmelse som kan träffa en viss informationsmängd och vilka övriga rättsliga krav som ställs på skyddet av informationen. Vid en riskanalys identifieras och värderas vidare risker där hänsyn tas till olika aspekter, såsom säkerhetsläget eller andra relevanta omständigheter som kan påverka skyddet, t.ex. förekomsten av underleverantörer och vilka säkerhetsåtgärder som ska vidtas av den part som anlitas vid utkontrakteringen.

Den typ av analyser, bedömningar och kravställningar som kan vara värdefulla att göra inför utkontrakteringar är ofta högst relevanta även inför den olämplighetsbedömning som ska göras när 10 kap 2 a § OSL tillämpas. Kravställningen som blir resultatet av ett sådant arbete blir väsentlig vid olämplighetsbedömningen eftersom säkerhetsåtgärderna som ska tillämpas

[1] SKR-koncernen har en mall för personuppgiftsbiträdesavtal som finns tillgängligt via SKR:s hemsida.

av leverantören kan ge förutsättningar för att upprätthålla en tillräcklig skyddsnivå även när uppgifterna hanteras utanför organisationen. Även de åtgärder som vidtas inom den egna organisationen inför en utkontraktering är relevanta för den bedömningen.

I den mån ett sådant systematiskt informationssäkerhetsarbete redan bedrivs inför utkontrakteringar ter det sig naturligt att använda sig av en liknande metodik vid den olämplighetsbedömning som ska göras enligt 10 kap. 2 a § OSL. Om det efter en bedömning enligt denna metodik kvarstår risker som inte kunnat åtgärdas kan det vara olämpligt att röja sekretessbelagd information, vilket i så fall innebär att sekretessen inte kan brytas med stöd av 10:2 a § OSL.

Sammanfattning

Eftersom det finns olika leverantörer som erbjuder vidareförmedlingstjänster går det inte att göra en generell bedömning av om det är olämpligt att skicka sekretessbelagd information via en sådan tjänst, utan det ska göras en allsidig bedömning i förhållande till den enskilde leverantören och hur dennes informationshantering förhåller sig till de utgångspunkter som nämns i lagens förarbeten och som sammanfattas ovan. (Prop. 2022/23:97, s. 17).

Det är dock viktigt att poängtera att det inte finns inte något generellt hinder emot att skicka även sekretessbelagd information via en vidareförmedlare inom Mina meddelanden. Vidare är de frågor som väcks ur sekretessynpunkt inte unika för just denna typ av utkontraktering. Viss typ av känslig information, t.ex. sådan som rör totalförsvaret (15:2 OSL) eller som är säkerhetsskyddsklassificerad enligt säkerhetsskyddslagen, kan dock vara olämplig att röja för en sådan leverantör. Ett sätt att hantera olämplighetsbedömningsbedömningen är att koppla samman den med sådant systematiskt informationssäkerhetsarbete som är värdefullt att genomföra inom en organisation, t.ex. inför utkontrakteringar.

Mer läsning

Såvitt avser skyddade personuppgifter bör Skatteverkets vägledning för offentliga aktörer följas. Enligt denna ses digitala brevlådor som en säker kommunikationskanal. Mina meddelanden bör därför kunna användas för kommunikation även med individer som har skyddade personuppgifter, under förutsättning att de förutsättningar som diskuteras i promemorian är uppfyllda.

En fördjupad diskussion finns i eSams vägledning och de riktlinjer som anges där kan användas som utgångpunkter i de fall det är svårt att bedöma om det är olämpligt att lämna ut information, trots att det endast sker för teknisk bearbetning och teknisk lagring för myndighetens räkning.