YTTRANDE

2021-05-05

Dnr 2021040026

Till
Infrastrukturdepartementet

Angående delbetänkandet Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering (SOU 2021:1)

I delbetänkandet redovisar it-driftsutredningen en kartläggning av statliga myndigheters it-drift. Utredningen redovisar också en rättslig analys av myndigheters förutsättningar att överlåta vissa arbetsuppgifter som innefattar sekretessbelagda uppgifter till privata tjänsteleverantörer (utkontraktering av it-drift). Utredningen presenterar två författningsförslag: ett förslag till sekretessbrytande bestämmelse i offentlighets- och sekretesslagen (OSL) om utkontraktering av it-drift och ett förslag om inskränkt meddelarfrihet.

Inera har beretts tillfälle att yttra sig över rubricerat delbetänkande. Med anledning härav vill Inera framföra synpunkter på utredningens överväganden om röjandebegreppet och den föreslagna sekretessbrytande bestämmelsen.

Allmänna synpunkter

Inera är positiv till utredningens förslag om en sekretessbrytande bestämmelse vid myndighets utkontraktering av it-drift till privata tjänsteleverantörer eller andra myndigheter, men kan inte tillstyrka författningsförslaget i sin helhet. Inera delar utredningens uppfattning att en myndighet som utkontrakterar it-drift som innefattar sekretessbelagda uppgifter i klartext har röjt dessa i sekretesshänseende för tjänsteleverantören eftersom de är i leverantörens förvar. Det ligger i sakens natur att utkontraktering minskar myndighetens kontroll över de utlämnade arbetsuppgifterna, och att den reella kontrollen ligger hos tjänsteleverantören. Det står helt klart när det rör sig om uppgifter i klartext.

Inera AB | Box 177 03, Tjärhovsgatan 21 B, 118 93 Stockholm | Tel 0771-25 10 10, info@inera.se, www.inera.se | Organisationsnummer 556559-4230

Med det sagt anser Inera att röjande inte nödvändigtvis föreligger i alla situationer av utkontraktering. En sådan situation föreligger om myndigheter vidtar åtgärder av sådant slag vid utkontraktering som syftar till att varken tjänsteleverantören eller någon annan utomstående ska ta del av uppgifterna. Inera delar således inte utredningens uppfattning att kryptering är en betydelselös omständighet vid bedömningen huruvida uppgifter är röjda. Tvärtom anser Inera att kryptering som innebär att myndigheten själv ensam förfogar över krypteringsnycklar och eventuella vidtar andra tekniska säkerhetsåtgärder är just sådana omständigheter där myndigheten inte räknar med att tjänsteleverantören eller någon annan utomstående ska komma att ta del av uppgifterna.

Inera anser således att ett röjande av uppgifter vid utkontraktering inte föreligger om vare sig tjänsteleverantören eller en tredje person med rimliga eller lagliga medel inte kan ta del av uppgifterna. Sådan är situationen om myndigheten förfogar över krypteringsnycklar men inte leverantören, s.k. Hold Your Own Key-lösning. I denna del anser Inera att OSL bör närma sig unionsrätten i allmänhet och begreppet ”personuppgifter” i synnerhet i EU:s dataskyddsförordning (dataskyddsförordningen). Inera befarar att med den uppfattning som utredningen förespråkar om röjandebegreppet, finns en risk för att utvecklingen av nya och starkare krypton både inom offentlig och privat verksamhet försvagas eller stannar av.

Inera anser att utredningens författningsförslag bör kompletteras med ett nytt tredje stycke som ger uttryck för att sekretess inte hindrar att en uppgift lämnas ut till ett företag eller en annan enskild eller till en annan myndighet om dessa eller tredje person saknar rimliga eller lagliga medel att ta del av uppgifterna. Om någon genom brottslig handling bereder sig åtkomst till sekretessbelagda uppgifter ska dessa inte heller anses röjda eftersom åtkomsten inte frivilligt lämnats av myndigheten.

Den intresseavvägning som utredningen föreslår i samband med att en utkontraktering aktualiseras lägger ett stort ansvar på myndigheter att väga olika intressen mot varandra. Inera anser att det är en komplex bedömning där olika omständigheter ska vägas in. Sådana bedömningar ställer höga krav på kompetens och erfarenhet hos myndighetens medarbetare, vilken kompetens inte alltid finns tillgänglig i mindre kommuner. Förslaget innebär förvisso inget nytt i denna del; även sekretessprövningar vid en begäran från allmänheten om utfående av allmänna handlingar är komplexa att bedöma för en myndighet.

Det finns således ett behov av vägledning och stöd. Om myndigheterna, statliga som såväl kommunala, inte får en tydlig ledning i hur de ska resonera vid själva intresseavvägningen, anser Inera att intresseavvägningen riskerar bli ett slag i luften och skapa samma osäkerhet som råder idag om rättsläget för utkontraktering av sekretessbelagda uppgifter till utländska leverantörer. Inera anser därför att en central

förvaltningsmyndighet ska utpekas och som ska göra övergripande intresseavvägningar för specifika och utbrett använda utländska molntjänster inom den offentliga sektorn alternativt stå till förfogande för myndigheter med knappa resurser för att genomföra en adekvat avvägning, t.ex. små kommuner.

Särskilda synpunkter

Röjandebegreppet

Inera är positiv till utredningens förslag om en sekretessbrytande bestämmelse vid myndighets utkontraktering av it-drift till privata tjänsteleverantörer eller andra myndigheter, men kan inte tillstyrka författningsförslaget i sin helhet.

Inera delar inte utredningens slutsats att en myndighets överlåtelse av arbetsuppgifter som innefattar sekretessbelagda uppgifter alltid innebär ett röjande. Av definitionen av sekretess framgår att sekretess är ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en handling eller på något annat sätt. Det innebär att röjande kan ske genom utlämnande. Det innebär dock inte att ett utlämnande alltid innebär ett röjande.

Med det synsätt som IT-driftsutredningen förespråkar skulle en tjänsteman från en myndighet som besöker en annan myndighet där verksamhet bedrivs som rör Sveriges säkerhet, och där denne får lämna ifrån sig mobiltelefon, dator eller annan elektronisk utrustning i ett avsett besöksskåp, anses ha röjt (utlämnat) den information som finns i utrustningen till myndigheten. Detta skulle innebära att man vid sådan myndighetssamverkan aldrig kan ta med sig någon egendom som kan innehålla sekretessbelagd information. Inera anser att så långt kan inte röjandebegreppet sträcka sig.

Det hindrar dock inte att det kan anses oaktsamt att på detta sätt lämna egendom innehållande information i någon annans vård och att detta kan medföra ett straffansvar. Särskilt gäller detta om den aktuella informationen är av känslig eller speciellt skyddsvärd natur. Då skulle det rentav kunna anses oaktsamt att hantera information på sådant sätt att man utsätter sig för ökad risk för att någon obehörigen tillgriper informationen genom brottslig handling och att informationens då anses röjd och utlämnad (jfr NJA 1991 s. 103).

Inera anser vidare att om ett utlämnande sker med stöd av en sekretessbrytande bestämmelse, en bestämmelse om överföring av sekretess eller om uppgiften omfattas av en sekretessbestämmelse eller lagstadgad tystnadsplikt hos mottagaren så är den sekretessbelagda uppgiften förvisso röjd, men inte nödvändigtvis obehörigen röjd. Det måste finnas en nyansering utifrån ett straff- och dataskyddsrättligt perspektiv huruvida röjandet i sig innebär ett behörigt eller obehörigt röjande, och att

röjandet därmed i vissa fall kan bli föremål för ett ansvarsutkrävande och i andra fall inte. I vart fall som en utgångspunkt. Inera utesluter inte att ett röjande även kan vara obehörigt trots att mottagaren omfattas av en sekretessbestämmelse eller en lagstadgad tystnadsplikt (jfr lagen om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter). En sådan omständighet får möjligen betydelse för utfallet av menprövningen så till vida att straffansvaret kan göra mottagaren mindre benägen att sprida informationen vidare, vilket gör att risken för skada blir lägre, vilket i sin tur kan gynnsamt påverka möjligheterna att lämna ut uppgifterna till en tjänsteleverantör.

Ett obehörigt röjande måste rimligen avse en situation där en myndighet lämnar ut en uppgift till något eller någon som inte är betrodd att ta del av uppgiften eller där omständigheterna är sådana att man kan räkna med att uppgifterna kan komma att röjas för obehöriga. Då blir det rimligt att anta att sekretess är ett förbud att röja uppgifter för någon obehörig och att röja inte är ett neutralt uttryck som ska jämställas med ett utlämnande. Snarare synes skillnaden mellan begreppen röja och utlämnande vara att utlämnandet innefattar mer aktiva åtgärder för att ge någon tillgång till information, medan röjande är mera passivt till sin natur och kan bestå i att uppgiften hanteras så att den kan åtkommas av någon. Som jämförelse kan nämnas 2 kap. 3 § säkerhetsskyddsförordningen (2018:658) varav framgår att ”behörig” att ta del av säkerhetsskyddsklassificerade uppgifter eller i övrigt delta i säkerhetskänslig verksamhet är, om inte något annat följer av bestämmelser i lag, endast den som bl.a. har ”bedömts pålitlig från säkerhetssynpunkt”.

Ett annat exempel utgör 6 kap. patientdatalagen (2008:355) som reglerar sammanhållen journalföring. Enligt bestämmelserna får två eller flera vårdgivare ta del av varandras vårdrelaterade uppgifter genom direktåtkomst. Bestämmelserna har kompletterats med en sekretessbrytande bestämmelse i 25 kap. 11 § 3 OSL. Eftersom det finns en potentiell teknisk åtkomst för alla vårdgivare till varandras uppgifter i ett system för sammanhållen journalföring, såvida uppgifterna inte är spärrade, så anses alla vårdgivares uppgifter som tillgängliggjorts i systemet förvarade enligt tryckfrihetsförordningen hos i vart fall anslutna vårdmyndigheter. Enligt utredningens synsätt är därmed alla vårdgivares vårdrelaterade uppgifter röjda för varandra.

Det råder emellertid enligt 25 kap. 2 § OSL en absolut sekretess hos en vårdmyndighet för uppgift om en enskilds personliga förhållanden som gjorts tillgänglig av en annan vårdgivare enligt bestämmelserna om sammanhållen journalföring i patientdatalagen, om förutsättningar enligt 6 kap. 3, 3 a eller 4 § samma lag för att myndigheten ska få behandla uppgiften inte är uppfyllda. Det är en laglig begränsning således. Den fråga som Inera ställer sig med utgångspunkt från it-driftsutredningens resonemang är om uppgifterna är röjda även i denna situation på grund av den potentiella tekniska åtkomsten. Inera återkommer nedan till situationer

där sekretessreglerade uppgifter, trots utlämnande, inte ska betraktas som röjda om varken tjänsteleverantören eller en tredje person med rimliga eller lagliga medel kan ta del av uppgifterna.

Av 25 kap. 2 § 2 stycket OSL framgår emellertid att om förutsättningar för en vårdgivare att få ta del av vårdrelaterade uppgifter hos en annan vårdgivare är uppfyllda eller myndigheten har behandlat uppgiften enligt nämnda bestämmelser tidigare, gäller sekretess, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men. Dessa krav anses enligt domstolspraxis inte behöva vara uppfyllda såvida tredje part begär ut uppgifter från alla vårdgivare som är anslutna till ett system för sammanhållen journalföring om ändamålet är forskning. I domstolspraxis har forskare kunnat utfå hälsorelaterade uppgifter från privata vårdgivare via en region som ingått i ett system för sammanhållen journalföring, se Kammarrätten i Jönköpings dom, mål nr 94-17. Enligt it-driftsutredningens synsätt är uppgifter från i vart fall andra vårdmyndigheter som ingår i systemet för sammanhållen journalföring i en sådan situation behörigen röjda för regionen. Det finns inga lagliga hinder för att ta del av uppgifterna hos andra vårdmyndigheter för ändamålet forskning, och hos dessa är uppgifterna behörigen röjda för regionen. Inera menar med detta exempel att det finns en uttrycklig reglering som gör att det röjande som uppstår mellan berörda vårdmyndigheter är behörigt, och att det därför är klarlagt på ett sätt som gör det förutsebart för den som skyddas av sekretessreglerna att dennes uppgifter kan komma att hanteras på detta sätt.

Av 18 kap 9 § OSL framgår bl.a. att sekretess råder för uppgift om chiffer, kod eller liknande metod, om det kan antas att syfte därmed är att underlätta befordran eller användning i allmän verksamhet av uppgifter utan att föreskriven sekretess åsidosätts. Bestämmelsen tar sikte på situationer när sekretessbelagda uppgifter hanteras av obehöriga utan att föreskriven sekretess åsidosätts. Inera tar denna bestämmelse till intäkt för att lagstiftaren förutsätter att det finns metoder och situationer där uppgifter lämnats till eller hanteras av obehöriga utan att de sekretessbelagda uppgifterna är röjda. Ett exempel som faller inom bestämmelsens tillämpningsområde är när sekretessbelagda uppgifter krypteras och lämnas ut till en tjänsteleverantör av en myndighet utan att krypteringsnycklarna överlämnas till leverantören.

På motsvarande sätt måste en myndighet få ett utrymme att kunna vidta tekniska skyddsåtgärder av uppgifter i syfte att inte tillåta mottagaren eller någon utomstående att ta del av utkontrakterade uppgifter. Inera anser att kryptering är en sådan åtgärd som innebär att uppgifter kan lämnas ut till och hanteras av en obehörig utan att uppgiften röjs, dvs. utan att föreskriven sekretess åsidosätts. Det förutsätter givetvis att myndigheten ensam förfogar över krypteringsnycklarna. Detta synsätt delas också

av rättsordningen genom den nyss nämna bestämmelsen i 18 kap. 9 § OSL och Försvarsmaktens föreskrifter om signalskyddstjänsten (FFS2021:1), jfr bilaga 1.

Om utredningens synsätt skulle få råda, att även krypterade uppgifter är röjda trots att myndigheten ensam förfogar över krypteringsnycklarna, innebär det att även fysiska handlingar skulle vara utlämnade och därmed också röjda om en myndighet hyr lokaler av en annan myndighet eller av en privat hyresvärd eftersom det alltid kommer att finnas en teoretisk och praktisk möjlighet för hyresvärden att ta del av uppgifterna då det sker i dennes lokaler. Det kan även tänkas att uppgifter som finns i ett kassaskåp eller en portfölj teoretiskt kan låsas upp av en obehörig även om uppgifterna befinner sig i utrymmen som ägs av eller kontrolleras av myndigheten. Poängen är dock att myndigheten i dessa fall aktivt vidtagit åtgärder – omständigheter – där man inte alls räknar med att hyresvärden eller någon annan ska ta del av uppgifterna, något som följer av Högsta domstolens dom i NJA 1991 s. 103.

Inera ställer sig därför frågande till varför Högsta domstolens resonemang i NJA 1991 s. 103 inte skulle kunna även appliceras i en digital miljö vid en bedömning av om en uppgift är röjd eller inte och beakta omständigheter typiska för den digitala miljön för att skydda eller förhindra att sekretessbelagda uppgifter röjs, såsom kryptering av sekretessbelagda uppgifter där bara myndigheten förfogar över krypteringsnycklarna. Inera vill i detta sammanhang framhålla betydelsen av att inte tillämpa olika principer eller juridiska modeller beroende på om uppgifter finns i analog eller digital form, och oavsett om uppgifter skapades igår, skapas idag eller kommer att skapas i morgon.

Med det sagt anser Inera att röjande inte nödvändigtvis föreligger i alla situationer av utkontraktering. En sådan situation föreligger om myndigheter vidtar åtgärder av sådant slag vid utkontraktering som syftar till att varken tjänsteleverantören eller någon annan utomstående ska ta del av uppgifterna. Ett typexempel är en myndighet som utkontrakterar eller transporterar sekretessbelagda uppgifter i krypterad form, men ensam förfogar över krypteringsnycklarna. Inera delar således inte utredningens uppfattning att krypterade uppgifter är en betydelselös omständighet vid bedömningen huruvida uppgifter är röjda. Tvärtom anser Inera att kryptering och andra tekniska säkerhetsåtgärder är just omständigheter i analogi med NJA 1991 s. 103 och 18 kap. 9 § OSL där myndigheten inte räknar med att tjänsteleverantören eller någon annan utomstående ska komma att ta del av uppgifterna.

Inera anser att ett röjande inte föreligger om vare sig tjänsteleverantören eller en tredje person med rimliga eller lagliga medel inte kan ta del av uppgifterna, såsom vid kryptering där myndigheten förfogar själv över krypteringsnycklarna eller när absolut sekretess hindrar åtkomst till uppgifter (se ovan). I denna del anser Inera att OSL bör närma sig unionsrätten i allmänhet och personuppgiftsbegreppet i synnerhet enligt dataskyddsförordningen. Av beaktandesats 24 i dataskyddsförordningen

framgår att personuppgiftsbegreppet är relativt och inte absolut. För att avgöra om en fysisk person är identifierbar bör man enligt beaktandesatsen beakta alla hjälpmedel som, antingen av den personuppgiftsansvarige eller av en annan person, rimligen kan komma att användas för att direkt eller indirekt identifiera den fysiska personen. För att fastställa om hjälpmedel med rimlig sannolikhet kan komma att användas för att identifiera den fysiska personen bör man beakta samtliga objektiva faktorer, såsom kostnader och tidsåtgång för identifiering, med beaktande av såväl tillgänglig teknik vid tidpunkten för behandlingen som den tekniska utvecklingen.

Inera menar att samma förhållningssätt som kommer till uttryck i beaktandesatsen skulle kunna appliceras på röjandebegreppet. Vinsten skulle bli ett välkommet närmande till unionsrätten och ett entydigt synsätt på uppgifter enligt OSL och personuppgifter enligt dataskyddsförordningen. Om kryptering appliceras på ”personuppgifter” finns det med all sannolikhet inte en möjlighet för en tjänsteleverantör att med rimliga eller lagliga medel ta del av uppgifterna (”personuppgifterna”) som utkontrakteras av en myndighet, om den senare behåller krypteringsnyckeln och skyddar den på ett säkert sätt. Uppgifterna blir inte heller ”personuppgifter” hos tjänsteleverantören enligt dataskyddsförordningen.

Om någon genom brottslig handling bereder sig åtkomst till sekretessbelagda uppgifter ska dessa inte heller anses röjda eftersom åtkomsten inte frivilligt lämnats av myndigheten.

Inera anser att konsekvenserna av utredningens uppfattning om röjandebegreppet beträffande krypterade uppgifter ovissa. Det kan finnas en risk för att utvecklingen av nya och starkare krypton både inom offentlig och privat verksamhet försvagas eller stannar av. En sådan teknikutveckling är homomorfa krypteringar som gör det möjligt att låta någon få ta del av krypterade uppgifter utan att behöva dekryptera dem. Hur påverkas utvecklingen av sådana krypteringsmetoder med utredningens uppfattning? Inera anser därför att utredningens författningsförslag bör kompletteras med ett nytt tredje stycke som ger uttryck för att sekretess inte hindrar att en uppgift lämnas ut till ett företag eller en annan enskild eller till en annan myndighet om dessa eller tredje person saknar rimliga eller lagliga medel att ta del av uppgifterna.

Sammanfattningsvis delar inte Inera bedömningen att ett utlämnande av uppgifter i samband med utkontraktering av it-drift alltid är en form av röjande eftersom det kan förekomma situationer där uppgifter kommer att finns hos en leverantör utan att de för den skull är röjda i OSL:s mening, och att en nyansering måste ske avseende huruvida de röjda uppgifterna är behörigen eller obehörigen röjda. En sådan nyansering skulle kunna kan åstadkommas genom den föreslagna sekretessbrytande bestämmelsen, varför Inera till övervägande del tillstyrker bestämmelsen med reservation för vad som anförs i detta yttrande och Ineras förslag till kompletterande bestämmelse.

Den sekretessbrytande bestämmelsens utformning

Inera utgår från att begreppet teknisk bearbetning och teknisk lagring även inkluderar alla tjänster som kan ingå i tillhandahållande av it-drift, t.ex. leverantörs sammanställning av uppgifter på begäran av den utkontrakterande myndigheten och som sammanställs i en exporterad fil (se Kammarrätten i Stockholms dom i mål nr 1296-20).

Inera anser att det behöver förtydligas att den sekretessbrytande bestämmelsen även kan tillämpas i förhållande till underleverantörer till det företag som en myndighet anlitar.

Den intresseavvägning som utredningen föreslår i samband med att en utkontraktering aktualiseras lägger ett stort ansvar på myndigheter att väga olika intressen mot varandra. Inera anser att det är en komplex bedömning där olika omständigheter ska vägas in såsom myndighetens intresse av att använda tjänsterna mot uppgifternas art och omfattning, intresset som sekretessen ska skydda, eventuell tystnadsplikt hos mottagaren och möjligheterna att lagföra brott mot sådan tystnadsplikt m.m. Sådana bedömningar ställer höga krav på kompetens och erfarenhet hos myndighetens medarbetare, vilken kompetens inte alltid finns tillgänglig i mindre kommuner. Förslaget innebär förvisso inget nytt i denna del; även sekretessprövningar vid en begäran från allmänheten om utfående av allmänna handlingar är komplexa att bedöma för en myndighet.

Det finns således ett behov av vägledning och stöd. Om myndigheterna, statliga som såväl kommunala, inte får en tydlig ledning i hur de ska resonera vid själva intresseavvägningen, anser Inera att intresseavvägningen riskerar bli ett slag i luften och skapa samma osäkerhet som råder idag om rättsläget för utkontraktering av sekretessbelagda uppgifter till utländska leverantörer. Inera anser därför att en central förvaltningsmyndighet ska utpekas och som ska göra övergripande intresseavvägningar för specifika och utbrett använda utländska molntjänster inom den offentliga sektorn alternativt stå till förfogande för myndigheter med knappa resurser för att genomföra en adekvat avvägning, t.ex. små kommuner.

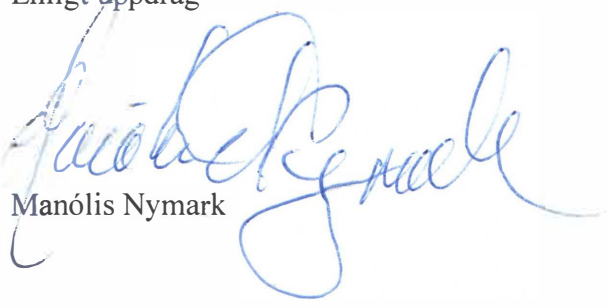
US CLOUD Act och liknande regleringar och 8 kap. 3 § OSL

Utredningen anser att det förhållandet att det finns en risk för att en privat tjänsteleverantör i enlighet med den lagstiftning som denne är bunden av (t.ex. US CLOUD Act eller någon liknande reglering) kan bli tvungen att lämna ut uppgifter till en utländsk myndighet innebär inte att den svenska myndigheten handlar i strid med 8 kap. 3 § OSL när den lämnar ut uppgifterna till tjänsteleverantören. Inte heller kan det bli fråga om ett otillåtet röjande enligt 8 kap. 3 § OSL om tjänsteleverantören i ett senare skede lämnar ut uppgifterna till en utländsk myndighet.

Inera anser att utredningen inte ger en tillräckligt nyanserad bild av frågan och ifrågasätter om detta verkligen är förhållandet om en tjänsteleverantör ägs till 100 procent av en utländsk stat eller dess myndigheter. I många stater är staten alltid delägare i landets företag. Är det då inte ett utlämnande till myndighet i strid med 8 kap. 3 § OSL om svensk myndighet anlitar en tjänsteleverantör som helt eller delvis ägs av en utländsk stat?

Beslut i detta ärende har fattats av verkställande direktören Peter Arrhenius. Föredragande har varit juristen Manólis Nymark. I handläggningen har deltagit chefsjuristen Sofia Klingensjö, dataskyddsombudet Fredrik Schölin, juristen Carl Stoltzman och it-strategen Richard Nilsson.

Enligt uppdrag



Manólis Nymark