YTTRANDE

Datum 2021-04-26
Ärendenummer 2021-POL000060

Remiss. Säker och kostnadseffektiv IT-drift - rättsliga förutsättningar för utkontraktering (SOU 2021:1)

Utredningens förslag i allmänhet

En säker och kostnadseffektiv it-drift är en förutsättning för den offentliga förvaltningens digitalisering. Statliga myndigheter, kommuner och regioner ansvarar för att verksamhetens it-driftslösningar stödjer en effektiv verksamhetsutveckling och uppfyller krav på säkerhet (säkerhetsskydd, sekretess och dataskydd) och kostnadseffektivitet.

It-drift kan i den offentliga förvaltningen bedrivas i egen regi, genom utkontraktering till tjänsteleverantör eller genom samordnad it-drift. Vilken it-driftslösning som är den mest lämpade beror på verksamhetens uppdrag och vilka uppgifter som hanteras i verksamheten. Utkontraktering av it-drift och användning av molntjänster är ett vanligt sätt för statliga myndigheter, kommuner och regioner att hantera sin it-drift.

Utredningen uppdrag är att skapa bättre förutsättningar för den offentliga förvaltningen att få tillgång till säker och kostnadseffektiv it-drift genom antingen samordnad statlig itdrift eller genom tydligare rättsliga förutsättningar för att kunna anlita privata leverantörer av it-drift. I anledningen av uppdraget föreslår utredningen två författningsförslag: ett förslag till sekretessbrytande bestämmelse i OSL om utkontraktering av it-drift och ett förslag om inskränkt meddelarfrihet.

Region Skåne ställer sig generellt bakom utredningens förslag, men konstaterar samtidigt att ytterligare förtydliganden behövs för att få en robust och modern lagstiftning samt en ändamålsenlig förutsättning för den offentliga förvaltningens digitalisering.

Sekretessbrytande bestämmelse i OSL

I 10 kap. 2 a § offentlighets- och sekretesslagen (2009:400), OSL, införs en sekretessbrytande bestämmelse som tar sikte på fall då uppgifter lämnas ut till företag eller en annan enskild (tjänsteleverantör) eller till en annan myndighet som har i uppdrag att utföra endast teknisk bearbetning eller teknisk lagring av de

Besöksadress: Rådhus Skåne, Västra Storgatan 12
Postadress: Region Skåne 291 89 Kristianstad
Telefon (växel): 044-309 30 00
E-post: region@skane.se
Internet: www.skane.se
Organisationsnummer: 23 21 00-0255

uppgifter som lämnas ut för den utlämnande myndighetens räkning. Ett utlämnande ska – enligt den föreslagna bestämmelsen – inte ske om övervägande skäl talar för att det intresse som sekretessen ska skydda har företräde framför intresset av utkontraktering.

Delbetänkandet föreslår en ny sekretessbrytande bestämmelse i offentlighets- och sekretesslagen det vill säga en bestämmelse om hur och till vem viss information får röjas. Genom förslaget till en ny sekretessbrytande bestämmelse skapas en möjlighet för myndigheter att under vissa förutsättningar få röja information till tjänsteleverantörer. Region Skåne är inte principiellt emot att en sekretessbrytande bestämmelse införs, utan ser det som en nödvändig och logisk följd i anledning av införandet av lag (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter.

Den föreslagna sekretessbrytande bestämmelsen tar dock enligt Region Skånes mening inte sikte på *all* form av outsourcing. Endast outsourcing i form av teknisk bearbetning eller teknisk lagring omfattas. Region Skåne anser inte heller att utredningen tillräckligt noggrant utrett vad som gäller för den så kallade röjande-frågan, när en uppgift från myndighet kan anses vara röjd i förhållande till tjänsteleverantör.

Särskilt om röjande-frågan

Delbetänkandet bedömer att en myndighet som utkontrakterar it-drift *har* lämnat ut de uppgifter som omfattas av utkontrakteringen till tjänsteleverantören. Detta gäller oavsett om omständigheterna när uppgifterna tillgängliggjordes tjänsteleverantören var sådana att myndigheten – t.ex. genom kryptering eller annan teknisk säkerhetsåtgärd – inte måste ha räknat med att tjänsteleverantören eller någon annan utomstående skulle komma att ta del av uppgifterna. Uppgifterna är enligt delbetänkandet röjda enligt offentlighets- och sekretesslagen eftersom utredningen ser ett utlämnande *per se* är en form av röjande.

Därmed tolkar utredningen sekretessdefinitionen som att information som utlämnats (utanför myndighetens gränser) *alltid* är röjd. Att röjandebegreppet i OSL ska tolkas på sådant sätt att ett röjande förutsätter att myndigheten kan räkna med, dvs. att det anses vara sannolikt, att någon hos mottagaren får del av en sekretessbelagd uppgift är en snäv tolkning.

Region Skåne ifrågasätter i denna del delbetänkandets tolkning av legaldefinitionen av sekretess enligt 3 kap. 1 § OSL och indirekt delbetänkandets definition av röjande. Delbetänkandet redogör i princip endast för en tolkning; att varje utlämnande medför ett röjande. Det finns dock flera andra tolkningsalternativ hur denna definition ska läsas, vilket inte utredningen verkar särskilt ha beaktat.

Just för det offentligas räkning när det gäller teknisk bearbetning och lagring av handlingar som innehåller känsliga personuppgifter kan en tolkning vara att det inte kan vara fråga om röjande av uppgifter i en handling. Detta eftersom det i 2 kap. 9 § tredje stycket och 2 kap. 13 § första stycket tryckfrihetsförordningen anges att en handling som förvaras eller överlämnats som ett *led i* teknisk bear-

betning eller teknisk lagring *inte* anses vara en allmän handling. I enlighet med tryckfrihetsförordningen är det nödvändigt att upprätthålla en tydlig myndighetsgräns mellan myndigheter samt i förhållande till exempelvis en tjänsteleverantör som agerar på uppdrag av en myndighet. Region Skåne anser att denna fråga bör utredas och förtydligas ytterligare.

En annan källa som har använts för vägledning avseende röjande-frågan är 20 kap. 3 § brottsbalken (1962:700) om brott mot tystnadsplikt. Med utgångspunkt i förarbeten och praxis på det straffrättsliga området har det skapats en uppfattning av att ett straffrättsligt olagligt beteende även utgör en gräns för definitionen av vad som anses vara ett röjande. I 2 kap. 1 § OSL finns en särskild lydelse som gäller både tjänstemän och myndigheter. Här framgår att ett röjande i den meningen är en tydlig handlingsdirigerande regel i förhållande till sekretessreglerna. För röjande krävs det därmed inte att de särskilda förutsättningar som anges i brottsbalken för straffansvar är uppfyllda. I anslutning till detta kan det även konstateras att de ansvarspåföljder som eventuellt kan aktualiseras vid ett uppenbart felaktigt utlämnande från myndigheten, i det fall utlämnande skett utan att en enskild tjänsteman agerat eller när de straffrättsliga förutsättningarna i övrigt inte föreligger, framförallt finns på dataskyddsregleringens område. Region Skåne hade gärna sett att utredningen i denna del blev tydligare och att flera olika aspekter på den så kallade röjande-problematiken togs upp och utreddes som en vägledning för offentlig förvaltning.

Region Skåne anser även att utredningens enahanda tolkning leder till konsekvensen att det inte finns något krav på att en person *faktiskt* tagit del av informationen för att den ska betraktas som röjd i lagens mening. Information anses vara röjd även om tjänsteleverantören omfattas av en tystnadsplikt enligt avtal eller lag. Region Skåne anser att utredningen inte beaktat att ofta medför en myndighets utkontraktering de facto att tjänsteleverantörens medarbetare som en nödvändig följd kommer att *kunna* ta del av uppgifter, utan att för den delen faktiskt ha gjort så.

Utredningens förhållningssätt medför också att information som är krypterad eller pseudonymiserad ska betraktas som röjd när den behandlas av en tjänsteleverantör. I sammanhanget är det enligt Region Skåne av stor vikt att särskilja frågan om information är röjd eller inte, från frågan om vilka *skyddsåtgärder* som myndigheten är förpliktigad att säkerställa för informationsmängden. Det finns, trots en sekretessbrytande bestämmelse som medför att informationen får röjas, krav på vilken nivå av informationssäkerhet som myndigheten ska implementera. Det är alltså inte ointressant att kryptera information oavsett om det har betydelse för röjandefrågan eller ej. Även denna aspekt anser Region Skåne måste utredas och förtydligas ytterligare.

Särskilt om så kallade tredjelandsöverföringar

Det är bara tillåtet att överföra personuppgifter till en mottagare i ett land utanför EU eller EES om det kan ske på någon av de grunder som anges i kapitel V i dataskyddsförordningen. Delbetänkandet bedömer att det utgör en överföring av

personuppgifter till tredjeland när en personuppgiftsansvarig eller ett personuppgiftsbiträde behandlar personuppgifter genom användning av utrustning som finns i tredjeland. Det saknar enligt utredningen betydelse hur lång eller kort tid som utrustningen används, och om uppgifterna är krypterade eller pseudonymiserade – det är ändå fråga om personuppgifter och en överföring av sådana uppgifter.

Av detta följer enligt utredningen att det inte krävs – för att det ska vara fråga om en överföring – att uppgifterna lämnas ut till tredje part. Det innebär att även om personuppgifterna hela tiden är under den personuppgiftsansvariges kontroll är det alltså fråga om en överföring när de förs över till tredjeland eller internationell organisation. Motsatsvis konstaterar utredningen att det inte är fråga om en tredjelandsöverföring när personuppgifter behandlas uteslutande inom EU, även om den personuppgiftsansvarige eller personuppgiftsbiträdet som behandlar personuppgifterna är bunden av tredjelands lagstiftning som innebär att denna kan åläggas att lämna ut uppgifter direkt till ett tredjelands myndigheter. Tredjelandsöverföringen sker i det fallet först i samband med att uppgifterna överförs till myndigheter eller annan mottagare i tredjeland. Utredningen konstaterar att detta kan ha betydelse vid valet av personuppgiftsbiträde. Det avgörande enligt detta perspektiv tycks alltså enligt Region Skånes bedömning av utredningen vara *var* servrarna är placerade och inte frågan om huruvida personuppgiftsbiträdet kan komma att omfattas av ett tredje lands jurisdiktion. Region Skåne anser att utredningen här behöver förtydliga ytterligare vad som konkret avses.

Utredningen konstaterar vidare att med hänvisning till Europeiska dataskyddsstyrelsens *Rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelsen med EU-nivån för skydd av personuppgifter* att det inte finns några ytterligare tekniska skyddsåtgärder som kan bidra till ett adekvat skydd vid användning av sådana tjänster som träffas av användningsfallet, när tredjelandets myndigheters rätt till tillgång till uppgifterna som överförs går utöver vad som är nödvändigt och proportionerligt i ett demokratiskt samhälle. Så blir exempelvis fallet där mottagarens personal aktivt behöver ta del av personuppgifter (t.ex. vid support) för att kunna utföra sitt uppdrag. Region Skåne noterar att EDPB;s rekommendationer är ett utkast som varit ute till publik konsultation och att det därmed inte går med säkerhet göra gällande hur exempelvis tillsynsmyndigheten skulle anse att det finns några adekvata skyddsåtgärder att vidta i enlighet med rekommendationen. Utredningen bör ha detta med i beaktande och konkretisera sin bedömning för det fall att rekommendationen förändras.

Enligt utredningens tolkning av Schrems II domen så är domstolens konstateranden avseende rättsläget i USA, vad gäller inskränkningar av grundläggande rättigheter och tillgången till rättsmedel och oberoende prövning, även giltiga i förhållande till övriga grunder för överföring av personuppgifter till USA enligt dataskyddsförordningen, då kravet på skyddsnivå är detsamma oavsett vilken

grund som tillämpas. Utredningen menar att det är svårt att se en situation där ytterligare skyddsåtgärder kan vidtas som läker de brister som EU-domstolen bedömt finns i amerikansk lagstiftning. Region Skåne ifrågasätter här ett sådant uttalande från utredningen och vill särskilt uppmärksamma att denna tolkning kan få långtgående konsekvenser och skapar en ytterligare osäkerhet då ställningstagandet i sig är ett antagande. Utredningens tolkning innebär i realiteten långtgående överväganden och ställningstaganden för myndigheter som utkontrakterar it-drift och där överföring till tredje land snarare är regel än undantag.

Region Skåne vill i anledning härav poängtera att dataskyddsförordningen i sig bygger på ett riskbaserat förhållningssätt. Den skyddsnivån som dataskyddsförordningen syftar till att garantera är inte på något sätt absolut eller statisk, utan grundar sig i varje enskilt fall på en risk- och proportionalitetsbedömning. Som stöd för detta kan hänvisas till bland annat ingresspunkt 4 till dataskyddsförordningen som anger att rätten till skydd för personuppgifter inte är en absolut rättighet utan ska vägas mot andra grundläggande rättigheter i enlighet med proportionalitetsprincipen. Ett riskbaserat förhållningssätt framgår även av bland annat artikel 24 i dataskyddsförordningen avseende den personuppgiftsansvariges ansvar (som ålägger personuppgiftsansvariga att genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och visa att behandlingen uppfyller kraven i förordningen med beaktande av bland annat riskerna med behandlingen) och artikel 32 avseende säkerhet i samband med behandling av personuppgifter (som anger den personuppgiftsansvarige och personuppgiftsbiträdet ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken med behandlingen). EU-domstolen gjorde i sin dom i Schrems II-målet också tydligt att det inte är uteslutet att subjektiva omständigheter kan beaktas. Tvärtom ansåg domstolen att en bedömning ska göras i varje enskilt fall och vid behov ska kompletterande skyddsåtgärder vidtas. EU-domstolens uttalande tyder snarare på att det därmed ska vara möjligt att anta ett riskbaserat förhållningssätt i detta avseende. Region Skåne vill med detta visa på att kostnadseffektiv it-drift inom offentlig förvaltning ställer höga krav på säkerhet, men får i sig inte innebära olika typer av inlåsningseffekter som regleringar och tolkningar skapar och som verkar vara utredningens avsikt.

Särskilt om begreppet ”teknisk bearbetning och lagring”

Att utredningen använder det nuvarande och etablerade begreppet ”teknisk bearbetning och lagring” kan tyckas som ett enkelt sätt att täcka in en stor del av de tjänster som utkontrakteras, men om begreppet i sin nuvarande form omfattar samtliga av de it-driftstjänster som myndigheter överlåter åt andra att utföra är fortsatt oklart.

Region Skåne anser därmed att det behövs en uppdaterad och modern definition av begreppet ”teknisk bearbetning och lagring” som grundligt definierar vad som omfattar och som tar ett avstamp i var it- och digitaliseringsutvecklingen befinner sig idag. Begreppet behöver uppdateras för att omfatta de it-tjänster som i dagsläget som levereras av både privata leverantörer och myndigheter

som inte träffas av begreppet, exempelvis supportpersonal som tar del av information vid fjärrstyrning.

Inskränkningar i meddelarfriheten

Delbetänkandet föreslår att meddelarfriheten enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen ska inskränkas för den krets av personer som träffas av tystnadspliktslagen. Region Skåne har inget att erinra mot detta för det fall föreslagen sekretessbrytande bestämmelse i OSL införs.

Behov av fortsatt utredning och förtydliganden

Som myndighet finns enligt Region Skåne ett starkt framtida behov och incitament av att fortsätta kunna både utkontraktera it-drift, använda molntjänster samt att bedriva viss it-drift i egen regi. Därmed är behovet angeläget av att de rättsliga förutsättningarna för utkontraktering tydliggörs på nationell nivå, genom exempelvis tydlig, uppdaterad och strukturerad definition av vad som avses med it-drift, teknisk bearbetning, lagring etc.

Några av de största hindren för säker it-drift är utöver ett oklart rättsläge, bristande informationsklassificering och avsaknad av kompetens inom it och säkerhet men också beställarkompetens. Att en utredning inom detta område lägger största vikt vid att förtydliga och konkretisera vid var tid gällande tolkning är ett grundläggande behov för att kunna skapa en säker och ändamålsenlig digital offentlig förvaltning.

I utredningens slutbetänkande som ska redovisas senast den 15 oktober 2021 ska förslag på samordnad statlig it-drift presenteras. Region Skåne är angelägna om tydliga och ändamålsenliga lösningar som gäller samtlig offentlig förvaltning då presenteras avseende såväl de säkerhetsmässiga som rättsliga förutsättningarna vad gäller samordnad och kostnadseffektiv it-drift på ett nationellt sätt.

Carl Johan Sonesson
Ordförande

Alf Jönsson
Regiondirektör