Regeringen

Dir. 2019:64

Kommittédirektiv

Säker och kostnadseffektiv it-drift för den offentliga förvaltningen

Beslut vid regeringssammanträde den 26 september 2019

Sammanfattning

En särskild utredare ska kartlägga och analysera statliga myndigheters behov av säker och kostnadseffektiv it-drift samt hur dessa behov tillgodoses. Utredaren ska vidare analysera säkerhetsmässiga och rättsliga förutsättningar för samordnad statlig it-drift och lämna förslag på mer varaktiga former för sådan it-drift, om det bedöms lämpligt ur ett säkerhetsperspektiv, och de författningsförslag som detta kräver. Utredaren ska också analysera de rättsliga förutsättningarna för statliga myndigheter, kommuner och landsting att med bibehållen säkerhet utkontraktera it-drift till privata leverantörer och vid behov lämna författningsförslag. Syftet med utredningen är att skapa bättre förutsättningar för den offentliga förvaltningen att få tillgång till säker och kostnadseffektiv it-drift genom antingen samordnad statlig it-drift eller tydligare rättsliga förutsättningar för att kunna anlita privata leverantörer av it-drift.

Uppdragen att kartlägga och analysera statliga myndigheters it-drift och den offentliga förvaltningens rättsliga förutsättningar för utkontraktering med bibehållen säkerhet, inklusive eventuella författningsförslag, ska redovisas senast den 31 augusti 2020. Uppdraget att föreslå mer varaktiga former för samordnad statlig it-drift ska redovisas senast den 31 maj 2021.

Bakgrund

It-drift i den offentliga förvaltningen

Begreppet it-drift har ingen tydlig avgränsning utan omfattar både fysisk hårdvara som servrar och datorer, och mjukvara som datorprogram och operativsystem. Digitalisering och it skapar förutsättningar för en rättssäker och effektiv verksamhet och leverans av god service till enskilda. Eftersom myndigheter ofta hanterar uppgifter som omfattas av sekretess eller är av integritetskänsligt slag ställs särskilda krav på myndigheternas it-verksamhet. It-driften inom den offentliga förvaltningen ska också uppfylla krav på säkerhetsskydd och informationssäkerhet.

It-drift i egen regi

Motiven för en myndighet att hantera sin it-drift i egen regi kan variera. I en del fall handlar det om att få kontroll över systemen och tätare kontakt mellan verksamheten och systemdriften. I andra fall kan det finnas säkerhetsmässiga fördelar, t.ex. att slippa kommunicera över öppna nätverk för att nå en tjänst. Säkerhetsmässigt kan det också vara enklare att integrera ett system i en myndighets befintliga it-miljö med de administrativa och tekniska säkerhetslösningar som redan används. Men it-drift i egen regi kan också medföra begränsningar. Det kan röra sig om låg skalbarhet, dvs. svårigheter att förändra kapacitetsutnyttjandet, låg potential för utveckling och sämre utbud av möjliga säkerhetslösningar. En myndighet med it-drift i egen regi kan också gå miste om stordriftsfördelar som kan följa av samordning eller utkontraktering av it-drift.

Samordnad it-drift

Ett alternativ till utkontraktering är att en myndighet får i uppdrag att helt eller delvis hantera it-drift åt en annan myndighet, s.k. samordnad it-drift. Exempel på sådan samordning är att Skatteverket hanterar it-driften åt bl.a. Kronofogdemyndigheten och Valmyndigheten och att Länsstyrelsen i Västra Götaland samordnar it-driften för samtliga länsstyrelser.

Ett annat exempel på samordnad it-drift är Försäkringskassans tidsbegränsade uppdrag att tillhandahålla samordnad och säker it-drift för vissa statliga myndigheter. Syftet med uppdraget är att pröva och utvärdera former för samordnad it-drift inom staten. Intresset för att ansluta sig till Försäkringskassans tjänster har varit stort bland de statliga myndigheterna, och Försäkringskassans uppfattning är att behovet av ett totalåtagande är omfattande

och angeläget (dnr Fi2017/03257/DF). Detta stärker uppfattningen i tidigare rapporter, dvs. att det finns ett stort intresse för samordnad it-drift bland statliga myndigheter (se bl.a. Statens servicecenter, En gemensam statlig molntjänst för myndigheternas it-drift, dnr Fi2016/00274/SFÖ). Samordnad it-drift skulle också kunna ge bättre förutsättningar för sådan samverkan mellan myndigheter som syftar till att utveckla och erbjuda gemensamma digitala tjänster till medborgare och företag.

Vid samordnad it-drift är det viktigt att poängtera att en myndighet alltid är ytterst ansvarig för att den information som lämnas ut får ett effektivt och ändamålsenligt skydd och i övrigt hanteras i enlighet med gällande rätt. Risker med bl.a. centralisering av flera myndigheters information behöver också beaktas.

Utkontrakterad it-drift

Begreppet utkontraktering används ofta för att beskriva när en verksamhetsutövare lägger ut drift, underhåll, skötsel eller liknande av en viss del av verksamheten till en utomstående leverantör. Utkontraktering har ingen legal definition och innebär inte heller någon tydlig avgränsning mellan olika organisatoriska enheter. Med utkontraktering av it-drift avses i dessa direktiv att en myndighet genom offentlig upphandling eller på något annat sätt uppdrar åt en privat leverantör att hantera hela eller delar av myndighetens it-drift.

Det kan finnas flera bakomliggande motiv till utkontraktering av it-drift. Det kan t.ex. röra sig om effektivitets- och besparingsskäl, men även att myndigheten vill dra nytta av säkerhetslösningar, expertkompetens, innovationer eller annan teknisk utveckling hos privata leverantörer. Även om utkontraktering av it-drift kan innebära fördelar för en myndighet, kan det också innebära säkerhetsrisker. Privata leverantörers affärsmodeller är ofta komplexa vilket kan göra dem svåra att överblicka och förstå. Det förekommer också att underleverantörer anlitas eller byts ut, att uppgiftsmängder hanteras utanför Sveriges gränser och att avtalsförhållandena är komplicerade. I sammanhanget är det viktigt att poängtera att en myndighet aldrig genom utkontraktering kan undandra sig sitt ansvar utan är ytterst ansvarig för att den information som lämnas ut får ett effektivt och ändamålsenligt skydd och i övrigt hanteras i enlighet med gällande rätt.

Säkerhetspolisen har framhållit att utkontraktering kan leda till att den mängd information som samlas hos en leverantör medför att leverantörens verksamhet sammantaget är av stor betydelse för Sveriges säkerhet. Säkerhetspolisen har också konstaterat att leverantören riskerar att bli ett attraktivt mål för bl.a. andra länders underrättelseinhämtning (Säkerhetspolisens årsbok 2017). Sådan centralisering, där flera myndigheters information samlas hos en leverantör, innebär en ökad riskexponering bl.a. för känsliga uppgifter. Samtidigt kan utkontraktering innebära att en myndighets informationstillgångar får ett bättre tekniskt och administrativt skydd än vad som skulle varit fallet om myndigheten hanterat sin it-drift i egen regi.

Rättsliga förutsättningar och säkerhet

Oavsett hur en myndighet väljer att anordna sin it-drift ställs den inför en mängd komplexa rättsliga frågor som måste hanteras. Vid utkontraktering kan myndigheten dessutom behöva ta ställning till vilka eventuella rättsliga konsekvenser den allt mer globaliserade marknaden får för hanteringen av myndighetens information, t.ex. om myndighetens informationstillgångar kommer att exponeras för andra staters rättsordningar och lättare bli åtkomliga för utländska myndigheter och organisationer eller andra aktörer.

Upphandling och avtal

Rätt använt är offentlig upphandling och avtalsförvaltning nyckelfaktorer som ger en myndighet goda förutsättningar att ta del av marknadens it-driftstjänster på ett kostnadseffektivt och juridiskt hållbart sätt (se t.ex. Nationella upphandlingsstrategin). På motsatt sätt kan t.ex. en icke strategisk upphandling av it-drift medföra ovälkomna och långdragna konsekvenser i form av inlåsningseffekter, leverantörsberoende, oförutsedda kostnader och obalanserade avtalsvillkor. Det ställs således höga krav på en myndighets verksamhets- och beställarkompetens samt förmåga att formulera ändamålsenliga avtalsvillkor och följa upp leverantörens hantering av de utkontrakterade tjänsterna. Upphandlingsmyndigheten tillhandahåller stöd och vägledning för upphandling och avtalsförvaltning (se bl.a. Avtalsförvaltning, vägledning nr 2, 2016). MSB har tagit fram en vägledning för att upphandla informationssäkert (MSB1177, november 2018).

Sekretess och dataskydd

En förutsättning för att en myndighet ska kunna samordna sin it-drift med en annan myndighets eller utkontraktera den är att bestämmelser om

sekretess och dataskydd inte hindrar att uppgifter lämnas ut till och behandlas av den mottagande myndigheten eller leverantören.

Bland myndigheterna råder i dag en viss osäkerhet i fråga om de rättsliga förutsättningarna för utkontraktering. Det gäller främst tolkningen av när en uppgift ska anses röjd enligt sekretesslagstiftningen, något som bl.a. kommit till uttryck i eSamverkansprogrammets rättsliga uttalanden om röjande och molntjänster och om röjandebegreppet enligt offentlighets- och sekretesslagen (VER 2018:57 och VER 2015:90). I Digitaliseringsrättsutredningens slutbetänkande uttrycks att det finns en oro över att uppgifter som lämnas ut till en privat leverantör kan komma att röjas i strid med sekretesslagstiftningen (SOU 2018:25 s. 106). Denna oro har förstärkts det senaste året till följd av att den amerikanska rättsakten The Clarifying Lawful Overseas Use of Data Act (CLOUD Act) trädde i kraft under våren 2018. CLOUD Act syftar bl.a. till att förenkla för amerikanska rättsvårdande myndigheter att få tillgång till vissa uppgifter som finns lagrade hos leverantörer som omfattas av den amerikanska jurisdiktionen, oavsett var uppgifterna finns rent geografiskt.

Om ett uppgiftsutlämnande inkluderar personuppgifter, behöver den utkontrakterande myndigheten också säkerställa att den behandling av personuppgifter som kommer att utföras är förenlig med dataskyddsregleringen. Här avses främst Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) samt lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning. Även myndighets- eller sektorsspecifika registerförfattningar kan aktualiseras.

En särskild utmaning för en utkontrakterande myndighet kan vara att bedöma om leverantören kan ge tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder så att behandlingen uppfyller kraven i dataskyddsförordningen, att den registrerades rättigheter skyddas och att uppgifter inte olovligen förs över till ett tredjeland, dvs. ett land utanför EU- och EES-området.

Säkerhetsskydd

Den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet eller omfattas av ett för Sverige förpliktande internationellt åtagande

om säkerhetsskydd (säkerhetskänslig verksamhet) omfattas av säkerhetsskyddslagen (2018:585) och de bestämmelser i förordning och föreskrifter som kompletterar lagen. Med säkerhetsskydd avses skydd av säkerhetskänslig verksamhet mot spionerі, sabotage, terroristbrott och andra brott som kan hota verksamheten samt skydd i andra fall av säkerhetsskyddsklassificerade uppgifter. Enligt säkerhetsskyddslagstiftningen gäller särskilda krav om en statlig myndighet avser att ge en leverantör tillgång till eller möjlighet att förvara säkerhetsskyddsklassificerade uppgifter av visst slag utanför myndighetens lokaler eller om leverantören kan få tillgång till vissa typer av säkerhetskänsliga informationssystem utanför myndighetens lokaler. En myndighet som t.ex. avser att utkontraktera hela eller delar av sin it-drift ska identifiera och dokumentera vilka uppgifter eller informationssystem som leverantören kan få del av och som kräver säkerhetsskydd och samråda med den berörda tillsynsmyndigheten innan ett sådant förfarande inleds. Tillsynsmyndigheten får förelägga myndigheten att vidta säkerhetshöjande åtgärder och ytterst besluta att myndigheten inte får genomföra utkontrakteringen. I betänkandet Kompletteringar till den nya säkerhetsskyddslagen (SOU 2018:82) föreslås bl.a. att denna reglering ska utökas och träffa alla aktörer som omfattas av lagen samt att tillsynsmyndigheterna ska ges utökade befogenheter. Betänkandet bereds för närvarande inom Regeringskansliet.

Informations- och cybersäkerhet

Det finns stora mängder information och it-system som är av avgörande betydelse för samhällets funktionalitet och säkerhet eller som innehåller integritetskänsliga uppgifter. Om känslig information förloras, stjäls, manipuleras eller sprids till obehöriga kan det få allvarliga följder, se Nationell strategi för samhällets informations- och cybersäkerhet, skr. 2016/17:213 med en senare kompletterande bilaga: Uppdatering om genomförandet av Nationell strategi för samhällets informations- och cybersäkerhet. Likaså kan störningar i funktionaliteten hos it-system få allvarliga följder för samhällsviktig verksamhet. Den som ansvarar för ett it-system måste utgå från att attacker kan riktas mot såväl systemets funktionalitet som den information som hanteras. Informationssäkerhet måste därför vara en självklar och integrerad del i allt arbete på alla nivåer. Säkerhetsåtgärder syftar till att skapa en mer robust informationshantering vid samhällets normaltillstånd och att hantera mer allvarliga störningar, kriser under höjd beredskap och ytterst krig.

En myndighet som står inför valet att samordna sin it-drift med en annan myndighets eller utkontraktera måste säkerställa att den information som kommer att lämnas ut är tillräckligt skyddad hos mottagaren och att kraven på tillgänglighet och funktionalitet uppfylls. Vid en bedömning av säkerhetsrisker behöver myndigheten bl.a. beakta riskerna med en allt högre grad av centralisering av den offentliga förvaltningens it-drift och informationstillgångar. Centralisering kan medföra att leverantören blir ett attraktivt mål för antagonistiska attacker (Informationssäkerhet – trender MSB779, januari 2015). Centraliserad it-drift kan också innebära risk för bredare skadeverkningar vid lyckade attacker mot systemfunktionalitet eller information.

Trots riskbilden kan samordnad it-drift eller utkontraktering ge bättre förutsättningar för samhällets informations- och cybersäkerhet. Samordnad drift kan t.ex. förenkla införandet av enhetliga säkerhetsnivåer och ge utökade möjligheter till kontroll och uppföljning. Därtill skulle svåråtkomlig kompetens kunna utnyttjas på ett mer effektivt sätt. Samordnad it-drift kan också underlätta införande och användning av andra gemensamma tjänster och metoder som kan resultera i ökad informations- och cybersäkerhet i samhället.

Uppdraget att kartlägga och analysera statliga myndigheters it-drift

Statliga myndigheters behov av säker och kostnadseffektiv it-drift

Det saknas en heltäckande bild av statliga myndigheters behov av säker och kostnadseffektiv it-drift och hur behoven tillgodoses i dagsläget. En konsekvens av detta är att det inte heller finns en klar kostnadsbild över statsförvaltningens sammanlagda utgifter för it-drift. Det saknas också övergripande analyser av vilka ekonomiska, rättsliga, säkerhetsmässiga och övriga konsekvenser samordning respektive utkontraktering av it-drift leder till för varje enskild myndighet och för den statliga förvaltningen som helhet i förhållande till it-drift i egen regi.

I syfte att klarlägga statliga myndigheters behov och hantering av säker och kostnadseffektiv it-drift behöver dessa frågor kartläggas och analyseras. Kartläggningen ska omfatta ett representativt urval av statliga myndigheter, försvarsmyndigheterna och Säkerhetspolisen undantagna. Kriterier som ska beaktas vid urvalet av de myndigheter som ska ingå i kartläggningen är bl.a. att de ska ha olika storlek och finansieringsform samt ha uppgifter inom olika verksamhetsområden. Kartläggningen ska klargöra hur de utvalda

myndigheterna hanterar sin nuvarande it-drift, vilka specifika och prioriterade behov myndigheterna har av att samordna eller utkontraktera it-drift samt vilka behov myndigheterna bedömer sig ha över de kommande åren. De kartlagda myndigheternas kostnader för it-drift ska redovisas. I denna del kan utredaren bl.a. ta utgångspunkt i Ekonomistyrningsverkets rapporter inom ramen för it-användningsuppdraget (se bl.a. ESV 2018:30). Där det finns relevanta jämförelseobjekt och avtal ska en jämförelse göras mellan kostnaderna för it-drift i egen regi och utkontraktering i förhållande till samordning av it-drift.

Det behöver också kartläggas i vilken utsträckning it-drift i egen regi och samordning respektive utkontraktering av it-drift kan svara mot de statliga myndigheternas behov av och krav på it-drift och andra närliggande tjänster. I detta sammanhang är det särskilt relevant att undersöka och jämföra i vilken utsträckning de olika it-driftsformerna förmår leva upp till rättsliga och säkerhetsmässiga krav, t.ex. krav på säkerhetsskydd och informationssäkerhet samt sekretess och skyddet för den personliga integriteten. Vidare ska utredaren, oavsett myndigheternas val av driftsform, kartlägga myndigheternas beställarkompetens och förmåga att identifiera vilka säkerhetskrav som ska ställas på it-drift. Utredaren ska också kartlägga myndigheternas förmåga att identifiera risker för inlåsningseffekter och möjlighet att dra nytta av teknisk innovation.

Den efterföljande analysen ska svara på vilka huvudsakliga behov olika typer av myndigheter har av samordning eller utkontraktering av sin it-drift. Det kan t.ex. röra sig om i vilken utsträckning myndigheter har behov av ett helhetsåtagande för drift och förvaltning respektive mer specifika åtaganden, t.ex. drift av särskilt krävande digitala tjänster som kräver viss expertkompetens. Det kan också röra sig om behov av att utkontraktera annan närliggande verksamhet såsom stöd vid utveckling och teknisk utrustning. Om behoven skiljer sig åt exempelvis för myndigheter av olika storlek eller inom olika sektorer, ska dessa redovisas. Analysen ska också redogöra för för- och nackdelar av olika driftsformer samt jämföra kostnadsbilden för samordning respektive utkontraktering av it-drift jämfört med it-drift i egen regi. För att tydligare redovisa de kartlagda myndigheternas sammanlagda utgifter för it-drift ska de kostnader som kvarstår på myndigheterna vid utkontraktering av it-drift framgå av kostnadsbilden. Eftersom myndigheterna bär det yttersta ansvaret även vid utkontrakterad it-drift ska även kostnader för att upprätthålla ändamålsenlig kompetens på myndigheterna beaktas.

Vidare ska analysen belysa eventuella skillnader samt för- och nackdelar vid samordnad it-drift med andra statliga myndigheter jämfört med utkontraktering till en privat leverantör. Det kan exempelvis gälla kvalitet, kontinuitet, riskhantering, säkerhet, skalbarhet, flexibilitet, transparens eller möjlighet att dra nytta av teknisk utveckling och digital innovation.

Utredaren ska därför

- kartlägga och analysera statliga myndigheters behov av säker och kostnadseffektiv it-drift, hur behoven är tillgodosedda och kostnaderna för dessa,
- kartlägga och analysera i vilken utsträckning olika it-driftsformer – i egen regi, samordning respektive utkontraktering – kan svara mot statliga myndigheters behov av och krav på it-drift, samt vilka förutsättningar myndigheter har för ändamålsenlig kravställning inom området, och
- analysera vilka behov av it-drift och närliggande tjänster hos statliga myndigheter, respektive olika verksamhetshetssektorer, som utifrån behovsanalysen är mest prioriterade att tillgodose.

Samordnad it-drift – omvärldsanalys

Det finns mycket att lära både av hur man nationellt och i andra länder har valt att hantera frågor om samordnad statlig it-drift och offentlig-privat samverkan kring it-drift. Dessa erfarenheter behöver kartläggas och analyseras för att det ska gå att bättre förstå vilka alternativ som står till buds och hur de olika lösningarna står sig mot varandra utifrån bl.a. säkerhet och kostnadseffektivitet, samt vilka utmaningar och problem de olika länderna har stött på. Finland har genomfört en större reform genom ökad centralisering och övergång till samordnad statlig it-drift genom myndigheten Valtori. Även Danmark och Norge har erfarenheter av samordnad statlig it-drift. Utanför Norden finns flera intressanta och relevanta exempel på såväl samordnad statlig it-drift som offentlig-privat samverkan kring molntjänster och it-drift. Tyskland har infört en lösning med en statlig molntjänst som hanterar it-drift för flera centrala myndigheter frikopplat från internet. Storbritannien har genom en gemensam molntjänstportal valt att samordna utkontraktering till kommersiella molntjänstleverantörer. I Sverige finns flera exempel på samordnad statlig it-drift som bör analyseras, t.ex. Skatteverkets hantering av it-drift åt Kronofogdemyndigheten och Valmyndigheten samt länsstyrelsernas samordnade it-drift. De lärdomar som dragits nationellt och i andra länder av samordnad statlig it-drift bör tas till vara och utgöra en del

av underlaget inför förslag om inriktning för en mer varaktig form av samordnad statlig it-drift i Sverige.

Utredaren ska därför

- kartlägga och analysera relevanta modeller för myndigheters it-drift såväl nationellt som i ett urval av särskilt intressanta länder med såväl samordnad statlig it-drift som offentlig-privat samverkan kring samordnad it-drift.

Uppdraget att föreslå mer varaktiga former för samordnad statlig it-drift

Försäkringskassans uppdrag om samordnad och säker statlig it-drift

De erfarenheter och den kompetens Försäkringskassan har byggt upp inom ramen för sitt uppdrag att tillhandahålla samordnad och säker statlig it-drift behöver tas till vara i det fortsatta arbetet att föreslå samordnad statlig it-drift. Försäkringskassans uppdrag behöver därför utvärderas och analyseras. Utredaren ska bl.a. redovisa hur Försäkringskassan byggt upp sin organisation kring de tjänster som tillhandahålls, för- och nackdelar med finansieringsmodell, hur anslutningsprocesserna med kundmyndigheterna har fortlöpt och om uppdraget i övrigt föranlett några särskilda utmaningar t.ex. när det gäller informationssäkerhet, säkerhetsskydd eller kund- och avtalsförvaltning. Utvärderingen ska innehålla en analys av vilka eventuella samordningsvinster och andra nyttor, t.ex. kostnadseffektivitet, ökad säkerhet, flexibilitet och skalfördelar, som kan uppnås vid samordnad statlig it-drift, i jämförelse med it-drift i egen regi respektive utkontraktering. Utredaren ska också redovisa vilka eventuella nackdelar som kan följa av samordnad statlig it-drift.

Utredaren ska därför

- utvärdera Försäkringskassans uppdrag att tillhandahålla samordnad och säker statlig it-drift och redovisa vilka slutsatser som kan dras i fråga om bl.a. upparbetad organisation, finansieringsmodell, tjänsteleverans, samordningsvinster samt påverkan på kärnverksamhet i fråga om bl.a. resursbehov och prioriteringar inom verksamheten, och
- analysera vilka lärdomar, erfarenheter och investeringar som är relevanta att vidareutveckla inom ramen för förslag till mer varaktiga former för samordnad statlig it-drift.

Säkerhetsmässiga och rättsliga förutsättningar för samordnad statlig it-drift

Samordning av statlig it-drift skulle innebära en allt högre grad av centralisering av den statliga förvaltningens it- och informationstillgångar, vilket leder till särskilda säkerhetsmässiga utmaningar. Många statliga myndigheter bedriver verksamhet som till någon del är av betydelse för Sveriges säkerhet och träffas därigenom av säkerhetsskyddslagen. I dessa fall är det säkerhetsskyddslagstiftningen som sätter ramarna för om det över huvud taget är möjligt för en myndighet att samordna eller utkontraktera sin it-drift. Även en aggregering av flera statliga myndigheters informationstillgångar kan leda till att information som fristående inte skulle bedömas falla inom ramen för säkerhetsskyddslagen ändå omfattas av lagen, då de samlade informationstillgångarna får en annan hotbild och ett annat skyddsvärde. Vidare ansvarar varje myndighet för att beakta och planera för totalförsvarets krav, i enlighet med vad som bl.a. föreskrivs i förordningen (2015:1053) om totalförsvar och höjd beredskap.

De säkerhetsmässiga för- och nackdelarna för statliga myndigheter att ansluta sig till samordnad it-drift jämfört med att hantera it-drift i egen regi eller utkontraktera driften behöver analyseras. Analysen bör bl.a. innehålla fördjupade resonemang om hur regelverken om säkerhetsskydd, informationssäkerhet, offentlighet och sekretess samt skyddet för den personliga integriteten kan upprätthållas och utvecklas.

Även de rättsliga förutsättningarna för samordnad it-drift i övrigt behöver genomlysas. I analysen ska särskilt fokus läggas på avtalsrättsliga förhållanden, bl.a. när det gäller statliga myndigheters förutsättningar att ingå rättsligt bindande avtal med varandra, ansvarsförhållanden och funktioner för ansvarsutkrävande, prioritering av driftbehov vid incidenter, avtalsförvaltning m.m. I analysen bör de avtalsmodeller som tagits fram inom ramen för Statens servicecenters tillhandahållande av tjänster beaktas. Det behöver vidare utredas om det finns konkurrens- och marknadsrättsliga förutsättningar för samordnad it-drift, hur statligt tillhandahållen it-drift förhåller sig till regelverken om offentlig upphandling och om det är nödvändigt att författningsreglera anslutning till sådan it-drift.

Utredaren ska därför

- analysera de säkerhetsmässiga förutsättningarna för samordnad statlig it-drift, särskilt när det gäller krav på säkerhetsskydd och informationssäkerhet samt sekretess och skyddet för den personliga integriteten,
- analysera de rättsliga förutsättningarna för samordnad statlig it-drift, särskilt när det gäller avtals- och upphandlingsfrågor samt konkurrens- och marknadsrättsliga frågor, och
- vid behov lämna författningsförslag som möjliggör att inrätta samordnad statlig it-drift.

Eventuella författningsförslag ska utformas med hänsyn tagen till kraven på säkerhetsskydd och informationssäkerhet, offentlighet och sekretess samt skyddet för den personliga integriteten. Om ändringar i offentlighets- och sekretesslagen föreslås ska de inte innebära någon förändring av lagens struktur och begreppsapparat. Inte heller ska sådana förslag innefatta ändring av, eller tillägg till, lagens bestämmelser om beslutsordning eller sekretessprövningens metodik. I uppdraget ingår inte heller att föreslå ändringar i grundlag eller i säkerhetsskyddslagstiftningen.

Samordnad, säker och kostnadseffektiv statlig it-drift

Utifrån resultatet av övriga delar av utredningen ska utredaren överväga vilka behov som finns av att inrätta mer varaktiga former av samordnad it-drift för den statliga förvaltningen samt om detta är lämpligt ur säkerhetssynpunkt. Utredaren ska också bedöma vilket tjänsteutbud som är mest prioriterat att tillhandahålla och beakta att samordnad it-drift ska vara säker, konkurrenskraftig och kostnadseffektiv.

Vidare ska utredaren analysera och ta ställning till vilka myndigheters it-drift som lämpar sig för samordning, och om vissa myndigheters it-drift på grund av säkerhetsmässiga förutsättningar eller särskilda myndighetsspecifika behov inte lämpar sig för sådan samordning.

Utredaren ska vidare lämna förslag på hur samordnad it-drift för den statliga förvaltningen kan organiseras och finansieras på ett kostnadseffektivt sätt. Här ingår att analysera om it-drift bör tillhandahållas av en ny eller befintlig myndighet eller om tjänsterna kan tillhandahållas av flera olika myndigheter, t.ex. utifrån sektorsspecifika behov. En utgångspunkt är att den kapacitet och de förmågor och erfarenheter som har byggts upp inom ramen för

Försäkringskassans pågående uppdrag att erbjuda samordnad och säker statlig it-drift ska tas till vara. Utredaren ska lämna alternativa och rangordnade förslag på organisationsmodeller, och med utgångspunkt i dessa även lämna förslag på en eller flera alternativa införandeplaner. Eventuella förslag som har övervägts men avfärdats ska redovisas och motiveras.

Utredaren ska också överväga om det bör vara obligatoriskt för delar av den statliga förvaltningen att ansluta sig till samordnad it-drift eller om anslutning ska grunda sig på frivillighet. Utredaren ska i denna del särskilt analysera konsekvenserna av obligatorium respektive frivillighet på inledande och avbrytande av it-driftssamverkan mellan myndigheterna samt rättsliga överväganden kopplat till detta. Vidare ska risker och konsekvenser för anslutande myndigheters specifika behov eller verksamhet vid införande av en obligatorisk anslutning särskilt analyseras, bl.a. risken att myndighetens kärnverksamhet blir lidande om myndighetens behov inte kan tillgodoses eller prioriteras av den myndighet som sköter it-driften. Det behöver även analyseras om det finns behov av särskilda prioriteringsmodeller eller -funktioner för anslutning med anledning av specifika eller brådskande behov hos vissa myndigheter.

Utredaren ska vid utformningen av förslagen beakta möjligheterna att använda privata leverantörer vid tillhandahållandet av samordnad it-drift för att dra nytta av fördelar i termer av säkerhet, teknikutveckling, innovationskraft och kostnadseffektivitet. Utredaren bör särskilt överväga om och hur kommersiella it-driftstjänster kan ingå i den samordnade it-driften. Det kan exempelvis vara i form av hybridlösningar där kommersiella it-driftstjänster används för att hantera hög belastning eller uppgifter som är mindre känsliga. Det kan också handla om lösningar där den aktör som tillhandahåller samordnad it-drift även upphandlar och samordnar användningen av kommersiella it-driftstjänster vid sidan av den samordnade statliga it-driften.

Utredarens förslag ska i samtliga delar grunda sig på en analys av säkerhetsmässiga, samhällsekonomiska och budgetära konsekvenser av att inrätta samordnad it-drift. I analysen ska det även ingå konsekvensbeskrivningar för det alternativet att it-driften inte samordnas, dvs. att varje myndighet fortsätter att ha it-drift i egen regi. När det gäller de säkerhetsmässiga konsekvenserna ska analysen beakta krav på säkerhetsskydd och informationssäkerhet samt sekretess och skyddet för den personliga integriteten såväl ur ett samhällsövergripande perspektiv som ur ett enskilt myndighetsperspektiv.

Analysen ska även beakta de krav som ställs mot bakgrund av att planeringen för totalförsvaret har återupptagits (prop. 2014/15:109, bet. 2014/15:FöU11, rskr. 2014/15:251). Utredaren ska också ta hänsyn till eventuella risker med centralisering av statsförvaltningens it-drift, geografisk placering och fysiskt skydd av datorhallar, potentiell exponering av myndigheters information mot andra länders rättsordningar samt risken för att informationen görs åtkomlig för obehöriga.

Utredaren ska därför

- analysera och lämna alternativa och rangordnade förslag på utformning och organisering av samordnad it-drift utifrån myndigheternas generella och specifika behov, tillsammans med införandeplaner,
- föreslå vilket tjänsteutbud som ska tillhandahållas inom ramen för samordnad it-drift, utifrån myndigheternas prioriterade behov,
- föreslå hur generella och myndighetsspecifika krav på informationssäkerhet och säkerhetsskydd kan tillgodoses,
- redogöra för om det finns vissa myndigheter eller typer av myndigheter, utöver försvarsmyndigheterna och Säkerhetspolisen, eller viss särskilt känslig information som inte bör hanteras inom ramen för samordnad it-drift,
- analysera om och föreslå hur privata leverantörer kan användas vid tillhandahållande av samordnad it-drift, och
- analysera och redogöra för budgetära, samhällsekonomiska och säkerhetsmässiga konsekvenser av de förslag som redovisas samt lämna förslag till finansiering.

Utredaren kan vid behov behandla sådana närliggande frågor som har samband med de frågeställningar som ska utredas, under förutsättning att uppdraget ändå bedöms kunna redovisas i tid samt att de eventuella förslag som läggs fram är finansierade.

Uppdraget att utreda rättsliga förutsättningar för utkontraktering till privata leverantörer

Utgångspunkten inom EU är att data ska kunna flöda fritt, vilket bl.a. kommer till uttryck i Europaparlamentets och rådets förordning (EU) 2018/1807 av den 14 november 2018 om en ram för det fria flödet av andra data än personuppgifter i Europeiska unionen (dataflödesförordningen). En statlig myndighet, en kommun eller ett landsting som avser att utkontraktera

it-drift till en privat leverantör, oavsett var denne är lokaliserad, måste dock beakta en mängd olika regelverk. Det gäller t.ex. sådana som rör offentlighet och sekretess, behandling av personuppgifter, arkivhantering, upphandling, informationssäkerhet och säkerhetsskydd samt upphovs- och avtalsrättsliga frågor. Behovet av säkerhetsskydd och informationssäkerhet är centralt.

Vid utkontraktering kan de rättsliga bedömningarna försvåras som en följd av t.ex. leverantörers komplexa affärsmodeller och en allt mer globaliserad marknad. Det gäller inte minst i fråga om kraven på hanteringen av sekretesskyddade uppgifter och bedömningen av när en uppgift ska anses röjd i offentlighets- och sekretesslagens mening. Samma sak gäller för hur det kan säkerställas att regelverket om dataskydd följs. I syfte att klargöra statliga myndigheters, kommuners och landstings möjligheter att anlita privata leverantörer behöver de rättsliga förutsättningarna för sådan utkontraktering kartläggas och analyseras.

Analysen ska bl.a. innehålla fördjupade resonemang kring kraven på hantering av sekretesskyddade uppgifter och risk för röjande av sekretessbelagda uppgifter. Här bör särskild vikt läggas vid frågan om huruvida avtalsreglerad tystnadsplikt och tekniska säkerhetsåtgärder, t.ex. kryptering eller pseudonymisering, kan påverka möjligheten att lämna ut uppgifter. Utredaren ska också särskilt analysera eventuella konsekvenser av att uppgifter som lämnas ut till en privat leverantör kan komma att exponeras för andra staters rättsordningar. Särskilt fokus ska ligga på betydelsen av rättsakter från tredjeland, t.ex. amerikanska CLOUD Act.

I uppdraget ingår också att analysera hur regelverket kring dataskydd kan uppfyllas, i synnerhet vid behandling av känsliga personuppgifter. I denna del ska särskild uppmärksamhet ägnas åt frågor som rör det organisatoriska och avtalsmässiga förhållandet mellan personuppgiftsansvarig och personuppgiftsbiträde, överföring av personuppgifter till tredjeland och skydd för den registrerades rättigheter.

Om utredaren finner att det finns lagstiftning som hindrar eller försvårar för statliga myndigheter, kommuner och landsting att utkontraktera it-drift till privata leverantörer, trots att säkerhetsmässiga, ekonomiska eller andra skäl talar för utkontraktering, ska detta redogöras för. Det kan också gälla omotiverade datalokaliseringskrav som ska upphävas enligt dataflödesförordningen.

Utredaren ska därför

- kartlägga i vilken utsträckning det förekommer lagstiftning som hindrar eller försvårar för statliga myndigheter, kommuner och landsting att, med bibehållen säkerhet, utkontraktera it-drift till privata leverantörer,
- analysera de rättsliga förutsättningarna för utkontraktering, och
- vid behov lämna författningsförslag som tydliggör förutsättningarna för sådan utkontraktering.

Eventuella författningsförslag ska utformas med hänsyn tagen till kraven på säkerhetsskydd, informationssäkerhet, offentlighet och sekretess samt skyddet för den personliga integriteten. Om ändringar i offentlighets- och sekretesslagen föreslås ska de inte innebära någon förändring av lagens struktur och begreppsapparat. Inte heller ska sådana förslag innefatta ändring av, eller tillägg till, lagens bestämmelser om beslutsordning eller sekretessprövningens metodik. I uppdraget ingår inte heller att föreslå ändringar i grundlag eller i säkerhetsskyddslagstiftningen.

Konsekvensbeskrivningar

Utredaren ska analysera de samhällsekonomiska effekterna i utredningsarbetets alla delar, från problembeskrivning och syfte till analys av alternativ och motiv till förslag. I den samhällsekonomiska analysen ska det även redogöras för konsekvenserna av status quo, dvs. att inte samordna myndigheternas it-drift. Utredaren ska vidare bedöma förslagens konsekvenser i enlighet med kommittéförordningen (1998:1474) och förordningen om konsekvensutredning vid regelgivning (2007:1244). I detta ingår att redogöra för ekonomiska konsekvenser för de enskilda myndigheter som direkt berörs av utredarens förslag. Om förslag lämnas som innebär en verksamhetsövergång eller avveckling av verksamhet, t.ex. för myndigheter som är direkt berörda av etableringen och tillhandahållandet av samordnad it-drift, ska de budgetära och verksamhetsmässiga konsekvenserna för detta särskilt analyseras. Vidare ska utredaren särskilt redogöra för eventuella marknadseffekter och konkurrenspåverkan för det privata näringslivet i förhållande till de potentiella samordningsvinster som kan uppnås av samordnad it-drift för hela eller delar av den statliga förvaltningen.

Kontakter och redovisning av uppdraget

Utredaren ska hålla Regeringskansliet (Infrastrukturdepartementet) informerat om det löpande arbetet.

Uppdraget ska utföras i nära dialog med Försäkringskassan och Myndigheten för digital förvaltning. Utredaren ska samråda med Myndigheten för samhällsskydd och beredskap, Försvarsmakten/MUST, Försvarets radioanstalt och Säkerhetspolisen när det gäller informationssäkerhetsfrågor och med Säkerhetspolisen, Försvarsmakten och Fortifikationsverket beträffande säkerhetsskydd och andra säkerhetsaspekter som t.ex. kan följa av centralisering av statliga myndigheters it-drift. I frågor som rör dataskydd ska utredaren samråda med Datainspektionen. Vidare ska utredaren samråda med de statliga myndigheter som är direkt berörda av utredningens förslag, t.ex. om förslagen omfattar verksamhetsövergång eller på annat sätt mer specifikt berör en enskild myndighet. I relevanta delar ska utredaren inhämta synpunkter från privata it-driftsleverantörer, it-branschen och Sveriges Kommuner och Landsting.

Utredaren ska under arbetets gång ta hänsyn och förhålla sig till det fortsatta arbetet med betänkandena Kompletteringar till den nya säkerhetsskyddslagen (SOU 2018:82) och Juridik som stöd för förvaltningens digitalisering (SOU 2018:25). Vidare ska utredaren särskilt beakta det arbete som bedrivs inom Utredningen om näringslivets roll inom totalförsvaret samt försörjningstrygghet i fråga om försvarsmateriel (dir. 2018:64) och inom Utredningen om samordning av statliga utbetalningar från välfärdssystemen (dir. 2018:50).

Uppdragen att kartlägga och analysera statliga myndigheters behov av it-drift och den offentliga förvaltningens rättsliga förutsättningar för utkontraktering ska redovisas senast den 31 augusti 2020. I delredovisningen ska utredaren redogöra för förslag till inriktning för det fortsatta utredningsarbetet när det gäller samordnad statlig it-drift. Uppdraget att förslå mer varaktiga former för samordnad statlig it-drift ska redovisas senast den 31 maj 2021.

(Infrastrukturdepartementet)