851 81 Sundsvall
0771-670 670
www.bolagsverket.se

2022-03-14

Betänkandet SOU 2021:97, Säker och kostnadseffektiv it-drift – förslag till varaktiga former för samordnad statlig it-drift

(I2021/03265)

Sammanfattning

Bolagsverket har inget att invända mot förslaget att statlig it-drift kan samordnas.

Bolagsverket är emellertid av uppfattningen att förslaget är så vagt forumlerat att det svårt att ta ställning till i detalj. Frågorna som behandlas i betänkandet behöver därför utredas ytterligare.

1.1 Förslag till förordning om samordnad statlig it-drift.

Bolagsverket anser att 8 § stycke 1 ska strykas. Leverantörsbegreppet bör hållas neutralt och inte kopplas till utpekade myndigheter. Särskilt utpekade leverantörsmyndigheter bör kunna anges i bilaga eller i en särskild förteckning hos samordnande myndighet.

Bolagsverket anser att 12 § stycke 2 ska strykas. Partsförhållandet mellan en leverantörsmyndighet och en anslutande myndighet bör inte regleras i förordningstext.

Bolagsverket anser att 12 § stycke 3 ska strykas. Den detaljstyrning som föreslås är inte önskvärd. Bolagsverket anser att rapporteringsskyldigheten enligt 18 § i förslag om förordning om samordnad statlig it-drift är tillräcklig.

Bolagsverket anser att 13-17 §§ ska strykas. Att ytterligare reglera personuppgiftsbehandling än vad som redan framgår av 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 och kompletterande bestämmelser till dataskyddsförordningen i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning kan i vissa fall vara lämpligt. Men i det här fallet tillför inte regleringen något ytterligare än vad som redan framgår av befintliga rättsakter och bör således tas bort.

10 Utgångspunkter och principer för varaktiga former för samordnad statlig it-drift

10.6. Säkerhet

I förslaget anges att säkerhet i en samordnad statlig it-drift omfattar såväl enskilda myndigheter som i den samordnade statliga it-driften som helhet. Med det menas säkerhetsskydd, informationssäkerhet, sekretess och dataskydd.

I SOU 2021:25, Struktur för ökad motståndskraft, föreslås bland annat att statliga myndigheter med ansvar inom en eller flera viktiga samhällsfunktioner och vars verksamhet

har särskild betydelse för krisberedskapen och totalförsvaret ska vara beredskapsmyndigheter. De myndigheter som ingår i den föreslagna strukturen med sektorer och särskilda beredskapsområden är myndigheter med ansvar inom en eller flera viktiga samhällsfunktioner och som har särskild betydelse för krisberedskapen och totalförsvaret. Det behöver inte vara myndigheter som är huvudman för verksamheter som träffas av krav på säkerhetsskydd utifrån säkerhetsskyddslagen (2018:585).

Av SOU 2021:25 framgår vidare att varje myndighet ansvarar för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt oaktat om Sverige befinner sig i en krigssituation eller i en fredstida kris.

Bolagsverket ser inte att något resonemang kring dessa särskilt utpekade myndigheter och deras it-system i den nu aktuella utredningen. Beredskapsmyndigheternas uppdrag omfattar även den interna styrningen och kontrollen. En effekt av att vara särskilt utpekad myndighet enligt beredskapsförordningen är att de system som hanterar samhällsviktig information kan omfattas av högre krav avseende informationssäkerhet och vem som får äga kontroll över systemen. Det framgår inte med tydlighet i hur det nu föreliggande förslaget förhåller sig till förslaget om en beredskapsförordning och de krav som lagts fram gällande dessa myndigheters informationssystem.

Vidare anser Bolagsverket att det bör tydliggöras att det även fortsättningsvis kommer vara möjligt för en myndighet att till en annan myndighet utkontraktera it-drift som innefattar hantering av säkerhetsskyddsklassificerade uppgifter, även om säkerhetsskyddsklassificerade uppgifter inte ska hanteras inom det nu föreslagna ordningen för samordning av det statliga tjänsteutbudet.

10.6.3

Det anges i utredningen att särskilda krav ställs på säkerheten i ett samordnat statligt tjänsteutbud där myndigheter erbjuder it-driftslösningr till andra myndigheter. Lösningen är enligt utredarna att det samordnade statliga tjänsteutbudet bör bygga på en flexibel och transparent lösning där it-driftstjänster från flera privata leverantörer ingår. Ur ett säkerhetsperspektiv bedöms enligt utredarna en sektorsindelning för anslutning inte vara lämplig.

Bolagsverket kan inte se förslag på kravställning avseende leverantörsmyndigheterna i utredningen. Myndigheter som väljer att utkontraktera sin it-drift är fortfarande ansvariga för sin data och för att datat hanteras i enlighet med gällande rätt. Det finns därför starka skäl till att införa exempelvis en certificeringsmekanism vilket får anses vara en kvalitetsstämpel på leverantörsmyndighetens säkerhetsarbete. De myndigheter som utkontrakterar sin it-drift ska följa ISO 27001. En sådan typ av systematiskt säkerhetsarbete bör även införas som krav för dem som utpekas som leverantörsmyndigheter av it-drift. Det krävs både kompetens och resurser för att bedöma om säkerhetsarbetet håller en adekvat skyddnivå vilket mindre myndigheter har svårt att klara av. Det leder till den oönskade effekten att de mindre myndigheterna hamnar i en situation där de måste lita på att leverantörsmyndigheterna uppfyller de krav som gäller för säkerhetsskydd, säkerhetsnivåer etcetera. En annan aspekt som bör tas i beaktande är dels den potentiella belastning som kan uppstå hos leverantörsmyndigheterna då varje myndighet som ska ta ställning till om utkontraktering ska ske kommer att behöva ta kontakt med

leverantörsmyndigheten och dels så behöver dessa leverantörsmyndigheter exponera sina säkerhetslösningar för alla myndigheter som innan beslut som utkontraktering kan tas ska säkerställa att det föreligger en adekvat skyddsnivå. Detta ansvar kan inte avtalas bort men förslagsvis kan ett tillitsramverk såsom exempelvis certifiering lösa en del av de frågor som uppstår vid en utkontraktering av it-drift.

En annan väsentlig del i informationssäkerhetsarbetet och då främst dataskydd är de risker som kan uppstå när leverantörsmyndigheten själv lägger ut it-driften på privata aktörer. Ägarförhållanden inom näringslivet är föränderliga. Det är inte osannolikt att ett företag får ett annat ägarförhållande och att driften plötsligt sker i ett tredje land där kravet på adevkata skyddsåtgärder inte är uppfyllda. Hur flyttar en myndighet tillbaka sin it-verksamhet i en sådan situation och är det ens möjligt? Att som personuppgiftsansvarig kräva att behandling omedelbart ska upphöra bör under sådana förhållanden vara omöjligt. Det är en lång kedja av aktörer och vem säkerställer att underbiträdet behandlar personuppgifter i enlighet med gällande regler för dataskydd? Uppföljningsansvaret för att behandlingen över tid är förenlig med gällande rätt ligger fortsatt hos den personuppgiftsansvarige.

11 Förslag till varaktiga former för samordad statlig it-drift

11.12 Utmaningar och risker med förslaget

Bolagsverket instämmer i bedömningen att det finns både utmaningar och risker med förslaget. Bolagsverket är emellertid av uppfattningen att vissa av dessa utmaningar och risker inte kan vänta och bör omhändertas innan beslut fattas om formerna för en samordnad statlig it-drift. En sådan utmaning är den styrmodell och administration som föreslås.

Förslaget bygger i huvudsak på ytterligare en infrastruktur som kommer kräva resurser på olika nivåer och då framförallt för Myndigheten för digital förvaltning. Att bygga en stor administration utan överväganden riskerar på sikt att belasta staten mer än nödvändigt. I begreppet kostnadseffektivet bör hänsyn tas till ett helhetsperspektiv, vilket inkluderar alla de delar som ingår i förslaget.

Utredningens förslag ger anledning att tro att styrformen varken leder till minskade kostnader för staten eller möjlighet för myndighetscheferna som ytterst sitter på beslutet att kunna fatta ett beslut på välgrundade underlag.

Bolagsverket är positiva till att förslaget bygger på frivillighet. Bolagsverket är av uppfattningen att framgången för statlig it-drift både kräver viss begränsning av myndigheternas valfrihet och samtidigt behöver ge myndigheterna viss valfrihet på lämplig nivå varvid flexibla lösningar bör vara utgångspunkt för fortsatt utredningsarbete.

12 Konsekvensutredning

12.5 Ekonomiska konsekvenser av förslagen

Incitamentet till förslaget är bland annat att samordning av it-drift ska vara kostnadseffektivt. Bolagsverket kan inte se att någon sådan beräkning eller kalkyl finns i betänkandet. Tvärtom framgår att förslaget bygger på frivillighet vilket leder till svårigheter att uppskatta vilka kostnader som kan uppstå hos berörda myndigheter. Bolagsverket har inga invändningar mot att lösningen finansieras via avgifter men med beaktande av de oklarheter som finns i förslaget har Bolagsverket svårt att ta ställning till om förslaget om en samordnad statlig it-drift är kostnadseffektivt, och att det därmed skulle vara bättre än att investera i kompetens inom den egna myndigheten.

Den administrativa lösningen som läggs fram talar enligt Bolagsverket för en kostsam och opraktisk hantering av utkontrakteringen och betänkandet saknar en beskrivning för hur DIGG ska agera som samordnare för den här typen av tjänster. De frågor som hanteras bör hanteras av dem med längst erfarenhet av it-drift, it-säkerhet och informationssäkerhet.

Det saknas viktiga delar i utredningen kring frågor som hur prioriteringar bör ske i verksamhetskritiska frågor. En sådan fråga är hur man tänker sig driften vid en fredstida kris.

De finns fördelar med förslaget. Det är uppenbart att det är svårt att rekrytera rätt kompetens inom it-området. Detta problem spänner över hela it-branschen från såväl it-drift till it-säkerhet. De kan därför finnas fördelar utifrån ett kompetensförsörjningsperspektiv.

12.2.3 Efterfrågan och utbud av samordnad statlig it-drift

Då anslutning bygger på frivillighet och det inte närmare preciseras vilka typer av nivåer, tjänster m.m som kan vara aktuell för samordning av statlig it-drift finner Bolagsverket att det är svårt att ta ställning till föreliggande förslaget.

I vissa situationer kan standardisering vara praktiskt, ekonomiskt och behövligt. När det kommer till ett så pass komplext område som it-drift där frågor kring både informationssäkerhet och it-säkerhet är avgörande kanske standardiserade eller helhetslösningar inte är efterfrågade. Myndigheter med utpekat ansvar enligt förslag om beredskapsförordning eller som har att följa säkerhetsskyddslagstiftningen har ett alldeles särskilt utpekat ansvar i dessa frågor vilket bör beaktas i ett fortsatt utredningsarbete.

Bolagsverket motsäger inte att det finns en efterfrågan på samordning av utkontraktering av it-drift. Däremot är Bolagsverket av uppfattningen att alla myndigheter inte har likadana behov och efterfrågan och kravställning är mer varierad än vad som framgår av utredningen. En fördel med förslaget är att samordning höjer lägsta nivån i det offentliga. efterfrågan av att få färdigpaketerade tjänster dvs. möjligheten att få välja vissa delar i ett tjänsteutbud snarare än utkontraktering av hela sin it-drift.

Detta yttrande har beslutats av generaldirektören Annika Stenberg. Deltagande i beslutet har varit direktören Inga Otmalm, rättschefen Erik Janzon, säkerhetsansvarige Mats Svärdsudd och avdelningschefen Joel Tostar.

Föredragande har varit verksjuristen Katarina Lindh.

Annika Stenberg

Katarina Lindh