Infrastrukturdepartementet
i.remissvar@regeringskansliet.se
i.esd.remisser@regeringskansliet.se
ingela.alverfors@regeringskansliet.se

Datum: 2021-05-07
Ert diarienummer: I2021/00342

Yttrande över remiss av SOU 2021:1 Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering

Amazon Web Services (AWS) tackar för möjligheten att yttra sig över delbetänkandet. Vi ser mycket positivt på att utredningen bringar klarhet i de rättsliga premisserna för utkontraktering av it-drift. Detta är en förutsättning för att offentlig sektor ska kunna dra nytta av molntjänster och dess fördelar: lägre kostnader, högre flexibilitet och starkare säkerhet. Vi välkomnar därför utredningens förslag till ny sekretessbrytande bestämmelse, som syftar just till att skapa sådan klarhet, och tillstyrker bestämmelsens föreslagna utformning i och för sig. Vi vill i övrigt lämna följande synpunkter.

Den föreslagna sekretessbrytande bestämmelsens omfattning

Vi tillstyrker som sagt den sekretessbrytandebestämmelsens utformning i utredningens författningsförslag. Vi anser dock att begreppet ”*teknisk bearbetning och lagring*” bör förtydligas. För att den sekretessbrytande bestämmelsen ska tjäna sitt syfte[1], och fullt ut tillgodose offentlig sektors stora behov av att kunna utnyttja hela utbudet av tillgängliga molntjänster, måste den vara tillräckligt brett utformad för att omfatta samtliga av de olika sätt som molntjänster levereras på, inklusive s.k. förvaltningstjänster och supporttjänster. Detta bör tydliggöras. Likaså bör det förtydligas att bestämmelsen omfattar teknisk bearbetning och lagring som vidtas av underleverantörer.

CLOUD Act och offentlighets- och sekretesslagen (OSL)

Vi delar utredningens bedömning att en myndighets röjande av uppgift för en tjänsteleverantör som omfattas av CLOUD Act inte innebär att myndigheten av den anledningen bryter mot OSL.

Röjandebegreppet

Utredningen gör bedömningen att ett utlämnande av uppgifter är en form av röjande, samt att det inte krävs att mottagaren av uppgiften ska ha tagit del av den

[1] SOU 2021:1, s. 193

för att den ska betraktas som röjd. Vi delar inte den bedömningen utan anser, i likhet med flera rättskunniga på området, att rättspraxis ger stöd för att ett röjande inte uppkommer bara för att en uppgift utlämnats till (t.ex. lagras hos) en it-leverantör, utan att frågan om uppgiften är röjd beror på sannolikheten för att t.ex. leverantörens personal ska *ta del av* uppgiften och de operativa, avtalsenliga och tekniska åtgärder, såsom kryptering, som kan mildra sannolikheten genom att göra uppgiften otillgänglig eller oanvändbar.[2] Med det sagt uppfattar vi att delbetänkandet i dess helhet, med det författningsförslag som det mynnar ut i, bringar det eftersökta förtydligandet av det rättsliga läget och gör det möjligt för offentlig sektor att utnyttja molntjänsters transformativa kraft.

Kryptering

Vi delar inte utredningens slutsatser i fråga om betydelsen av kryptering i sammanhanget, såsom att kryptering *"medför alltså endast att det blir mer osannolikt att tjänsteleverantören tar del av uppgifterna i jämförelse med vad som skulle ha varit fallet om åtgärderna inte hade vidtagits"*.[3] Det är viktigt att förstå både den tekniska aspekten av kryptering som gör att data inte kan tas del av i läsbar form, samt hur man som myndighet implementerar åtgärder för att få ut det mesta av krypteringslösningen. Om detta görs på ett riktigt sätt så är inte kryptering endast ett sätt att försvåra för obehörlig tillgång till data, utan det ger ett fullgott skydd.[4] Då detta är en sakfråga, och inte föremål för juridisk tolkning, hade vi önskat se den tekniska verkligheten bättre återspeglad i delbetänkandet.

Vi önskar även att utredningen hade gått in mer i detalj kring vilka överväganden myndigheter bör göra när de använder kryptering som verktyg. Vi uppfattar att vägledning behövs för att stödja myndigheter i detta arbete, särskilt eftersom förekomsten av kryptering och andra tekniska skyddsåtgärder kommer att tillmätas betydelse i den intresseavvägning som myndigheter ska göra inför beslut kring uppgifters utlämnande. Sådan vägledning bör omfatta ett antal viktiga frågor, såsom:

i) *Vem har tillgång till krypteringsnyckeln*? Myndigheter kan välja att separera tillgången till nycklarna ifrån tillgången till data. Detta görs genom att hantera nycklar i ett nyckelhanteringssystem vilket ytterligare försvårar möjligheten att få tillgång till det som krävs för att kunna bryta krypteringen på data. Sådana system kan vara från en annan leverantör.

---

[2] Synchs memorandum om CLOUD Act, s. 17
Cirios rapport "Molntjänster, offentlighet och sekretess i offentlig sektor", s. 12
Opinion av advokat Erik Brändt Öfverholm i *Dagens Samhälle*, 6 september 2019

[3] SOU 2021:1, s. 1282

[4] För mer detalj om hur kryptering tillämpas i praktiken, se:
https://aws.amazon.com/blogs/security/importance-of-encryption-and-how-aws-can-help/

ii) *När bör kryptering göras*? Kryptering kan och bör ske både vid transport och i vila. De tjänster som lagrar information bör tillhandahålla krypteringsmöjligheter som del av tjänsten.

iii) *Vilken krypteringstyp bör användas*? Vilken nivå av kryptering man väljer bygger naturligtvis på vilken skyddsnivå det man vill skydda har, men med moderna tjänster som hanterar kryptering utan några signifikanta prestandaförluster finns det ingen anledning att inte använda de starkaste kommersiellt tillgängliga krypteringstyperna såsom AES-256.

Tredjelandsöverföringar & EU-domstolens avgörande i mål C-311/18 (Schrems II)
Vi konstaterar att innebörden av Schrems II och dess betydelse för tredjelandsöverföringar av personuppgifter (och däribland frågan om vilka ytterligare skyddsåtgärder som därvid kan användas) alltjämt är föremål för tolkning och utredning av både Europeiska kommissionen och Europeiska dataskyddsstyrelsen. Det finns därför, enligt vår mening, skäl att avstå från att i utredningen dra definitiva slutsatser i dessa frågor.[5]

Hinder för säker it-drift
Utredningens kartläggning visar att de största hindren för säker it-drift utgörs av bristande informationsklassificering tillsammans med avsaknad av relevant kompetens inom verksamheten.[6] Informationsklassificering krävs för att kunna avgöra om uppgifterna är sekretessbelagda eller ej, och därmed om den föreslagna sekretessbrytandebestämmelsen är tillämplig. Vi önskar därmed att utredningen hade föreslagit någon lösning för hur myndigheter ska komma över dessa hinder för säker it-drift – t.ex. om vägledning som ger underlag och underlättar för myndigheterna i dessa bedömingarna.

[5] Jfr slutsatsen att ”[...] det inte finns ytterligare skyddsåtgärder som skulle tillåta överföring av personuppgifter till tredjeland som kan vidtas som läker de brister som EUdomstolen i Facebook Ireland och Schrems bedömer finns i amerikansk lagstiftning..” på sida 225, SOU 2021:1
[6]SOU 2021:1, s. 78