Adekvansbeslut och ny sekretessbrytande bestämmelse– grönt ljus för amerikanska molntjänster?

Slutsats

Ett beslut om adekvat skyddsnivå för personuppgifter för USA innebär inte ett förbehållslöst grönt ljus för amerikanska molntjänster. En myndighet måste ta hänsyn till alla lagkrav och verksamhetsbehov vid val av tjänster, dvs. tjänsterna måste uppfylla krav på såväl laglighet som säkerhet och lämplighet. Det är även konsekvensen av förslaget till ny sekretessbrytande bestämmelse.

Bland annat behöver följande beaktas:

- Risk för att inte kunna upprätthålla digitala tjänster vid kris och krig
- Risk för att inte kunna använda it-tjänsten i det dagliga arbetet
- Risker med samlad information eller att myndigheter blir beroende av en och samma leverantör
- Risker med dolda säkerhetsproblem

Att ta ställning till möjligheten och lämpligheten att använda sig av en viss molntjänst är utmanande eftersom juridik, teknik och hotbild är under ständig utveckling. Därför ger samverkan ett stort värde exempelvis genom att samarbeta om bedömningar av molntjänster. Minst lika värdefullt är samverkan om att gemensamt tydliggöra och förklara kravbilden för marknaden, det har arbetet inom dSam bevisat.

Som enskild myndighet och i samverkan behöver ett systematiskt arbete ske för att säkerställa att använda molntjänster är lagliga, säkra och lämpliga. Då bidrar vi till en uthållig digitalisering.

Syfte och målgrupp

Detta dokument som tagits fram av eSams molngrupp, vänder sig till medlemsmyndigheternas beslutsfattare och syftar till att utgöra stöd för myndigheternas bedömning av molntjänster.

Underlaget syftar inte till att vara en juridisk konsekvensanalys, här hänvisas till det arbete som expertgrupp Juridik bedriver. Syftet är att sätta adekvansbeslut och den nya sekretessbrytande bestämmelsen i en större kontext.

Nytt adekvansbeslut och ny sekretessbrytande bestämmelse

Det förväntas att EU-kommissionen kommer fatta ett nytt beslut om adekvat skyddsnivå avseende USA.[1] Det är mycket positivt att EU och USA med gemensamma ansträngningar arbetar för att underlätta flödet och skyddet av personuppgifter.

Det finns också ett förslag om en ny sekretessbrytande bestämmelse[2] som föreslås träda i kraft den 1 juli 2023. Bestämmelsen syftar till att ge förutsättningar för myndigheter att utkontraktera eller samordna sin it-drift.

Även om båda dessa förändringar träder i kraft finns det aspekter som myndigheter behöver beakta vid bedömning av molntjänster. I följande exempel belyser eSams molngrupp ett urval av dessa aspekter utan rangordning eller viktning.

Exempel - Digitala tjänster i kris och krig

Om en leverantör ska tillhandahålla digitala tjänster till myndigheter, måste myndigheten säkerställa att leverantören garanterar att tjänsterna kan upprätthållas vid kriser, gråzonsproblematik[3] (ett tillstånd mellan fred och krig) och krig.

Ett exempel på detta är finska statens anskaffning av en molntjänst för möten och chatt för 80 000 användare[4]. I kravställningen har angetts att tjänsten ska fungera oavsett om Finland förlorat tillgång till internet mot omvärlden.

Ett motsatt exempel är Ukraina som under pågående krig lade upp digital myndighetsinformation i molnet vid den ryska invasionen[5]. Syftet var att säkerställa informationens fortlevnad.

---

[1] Ett beslut om adekvat skyddsnivå innebär att personuppgifter får föras över till tredjeland utan ytterligare skyddsåtgärder som avtalsklausuler eller liknande. Syftet med reglerna om tredjelandsöverföring är att de registrerade ska garanteras en likvärdig skyddsnivå som i EU/EES för att värna om deras grundläggande fri- och rättigheter. När det gäller adekvansbeslutet avseende USA kommer det att gälla endast de organisationer som själva förklarat att de vill efterleva ramverket. Det gäller alltså inte generellt för all överföring till USA.
[2] En ny sekretessbrytande bestämmelse föreslås införas i offentlighets- och sekretesslagen (OSL), 10 kap. 2 a §, Prop. 2022/23:97 Sekretessgenombrott vid utlämnande för teknisk bearbetning eller teknisk lagring av uppgifter. Bestämmelsen gör det tillåtet för myndigheter att lämna sekretessbelagda uppgifter till en enskild eller till en annan myndighet som har i uppdrag att tekniskt bearbeta eller tekniskt lagra uppgifterna för myndighetens räkning. En uppgift får dock inte lämnas om det med hänsyn till omständigheterna är olämpligt. S.k. ”meddelarfrihet” slopas för den som omfattas av tystnadsplikt av teknisk bearbetning eller lagring av uppgifter.
[3] https://sv.wikipedia.org/wiki/Gr%C3%A5zon_%28nationellt_tillst%C3%A5nd%29
[4] https://elisavidera.com/ideas/valtori/
[5] https://news.microsoft.com/en-cee/2023/01/20/how-technology-helped-ukraine-resist-during-wartime/

Gemensamt för exemplen är att myndigheters planering för krisberedskap och totalförsvar inte separeras från försörjningen av digitala tjänster.

Exempel - Risk för att tjänsterna inte uppfyller de dagliga behoven

Medarbetare på en myndighet behöver kommunicera med varandra och utbyta dokument i ärenden av vitt skilda slag. Till det behövs tjänster för chatt, dokumenthantering, e-post, ordbehandling och videomöten som är rättsligt och tekniskt användbara för all typ av information som ska hanteras.

Efter informationsklassning och riskbedömning visar sig många molntjänster bara kunna användas till helt öppen information. Det minskar användbarheten och kräver att myndigheten skaffar ytterligare system med tillräckliga skyddsåtgärder för personuppgifter och sekretess. Den till synes enkla lösningen att använda en molntjänst gör då arbetet mer komplicerat för den myndighetsanställde som hela tiden måste bedöma vilken information som kan hanteras i vilken tjänst. Det uppstår också en risk att man använder tjänsterna överdrivet försiktigt, vilket i sin tur innebär produktionsförlust, osmidiga processer och dålig arbetsmiljö. Omvänt minskar osäkerheten med molntjänster som uppfyller högre säkerhetskrav. Det blir enklare för den myndighetsanställde att arbeta effektivt, lagligt och säkert.

Ett återkommande förslag från leverantörer är att skydda uppgifter via kryptering, men detta försämrar normalt sett molntjänsternas funktionalitet. Det kan dessutom vara svårt att bedöma om krypteringen är tillräcklig eller fungerar så som man tror. Till exempel måste krypteringen hålla hela informationens livslängd, och detta kan vara mycket svårt att garantera. Bland annat Googles VD har påtalat att underrättelsetjänster kan samla in specifik krypterad data som man tänker sig att kunna dekryptera i framtiden, när tekniken förbättrats och det finns nya tekniska möjligheter som saknas idag.[6]

Exempel - Begränsad riskspridning

Molnmarknaden domineras idag av en handfull globala leverantörer vars tjänsteutbud blir allt större och diversifierat. Respektive leverantörs utbud baseras i regel på deras egen teknik. Konsekvensen är att det blir utmanande att byta leverantör. Myndigheter lider av att it-marknaden många gånger saknar hälsosam konkurrens. Idag har över 50 % av kommuner och regioner samma e-posttjänst och samma leverantör som levererar mötestjänster[7]. Myndigheter hamnar lätt i fällan att välja en molntjänst som ingår i den

[6] https://www.foreignaffairs.com/united-states/eric-schmidt-innovation-power-technology-geopolitics
[7] https://webperf.se/articles/mejltjanster-offentlig-sektor/

licens som redan är inköpt utan att fundera över konsekvenserna. Med ett gemensamt beroende till en och samma leverantör, blir offentlig sektor sårbar utifrån svensk digital suveränitet. Det är långsiktigt fördelaktigt med en marknad där leverantörer använder öppna standarder. Det gör det enklare att byta leverantör och förenklar samverkan mellan olika leverantörers produkter.

Myndigheter måste kunna upprätthålla rådighet över sin data. Det förekommer att ägarvillkoren för data som används i tjänsten är otydliga och svåröverblickbara. Det kan gälla till exempel villkor vid avtalets upphörande. En myndighet måste kunna bestämma på vilket sätt tjänsten tillhandhålls och att det finns valmöjligheter, exempelvis molntjänst, via lokal leverantör eller egen it-drift. En myndighet behöver beakta långsiktiga gemensamma inlåsningseffekter och riskerna med att lägga ”alla ägg i samma korg”.

Exempel - Fördelar och nackdelar med att samla flera myndigheters information på ett och samma ställe

En myndighet planerar att ta fram en molntjänst som bygger på artificiell intelligens, som även ska kunna användas av andra myndigheter. Ju fler som använder tjänsten desto bättre fungerar den samtidigt som nyttan kommer fler organisationer till gagn.

Det är dock viktigt att komma ihåg att större sammantagna informationsmängder innebär en högre riskbild och ökar behovet av skydd. Ett sätt att minska risken är att begränsa användningsområdet och därmed informationsmängden. Vidare är det viktigt att ansvarsförhållandena för den samlade aggregerade informationen görs tydlig för alla involverade.

Exempel - Dolda säkerhetsproblem

Det finns flera exempel på kända it-lösningar med säkerhetsproblem. Det kan vara dold informationsinsamling i syfte att infiltrera eller spionera. En amerikanskägd tjänst som utvecklas i ett land med inkräktande cyberlagar innebär en motsvarande riskbild. Detta kan gälla AI[8], mobiltelefonbackup, sökmotorer, appar[9], sociala medier osv. Det kan upplevas svårt att göra bedömningarna och hantera att förutsättningarna kan förändras över tid. Trots det är det viktigt att dessa perspektiv beaktas.

[8] https://www.bloomberg.com/news/articles/2023-05-02/samsung-bans-chatgpt-and-other-generative-ai-use-by-staff-after-leak#xj4y7vzkg
[9] https://www.svd.se/a/QonX6P/tiktok-forbjudet-hos-flera-myndigheter

Fördjupat stödmaterial för analys av molntjänster

Det här underlaget tar upp och exemplifierar aspekter och situationer som kan behöva beaktas när molntjänster övervägs. För att ytterligare stödja medlemsmyndigheternas systematiska arbete planerar eSams molngrupp med start till hösten ta fram ett fördjupat stödmaterial för analys av molntjänster.