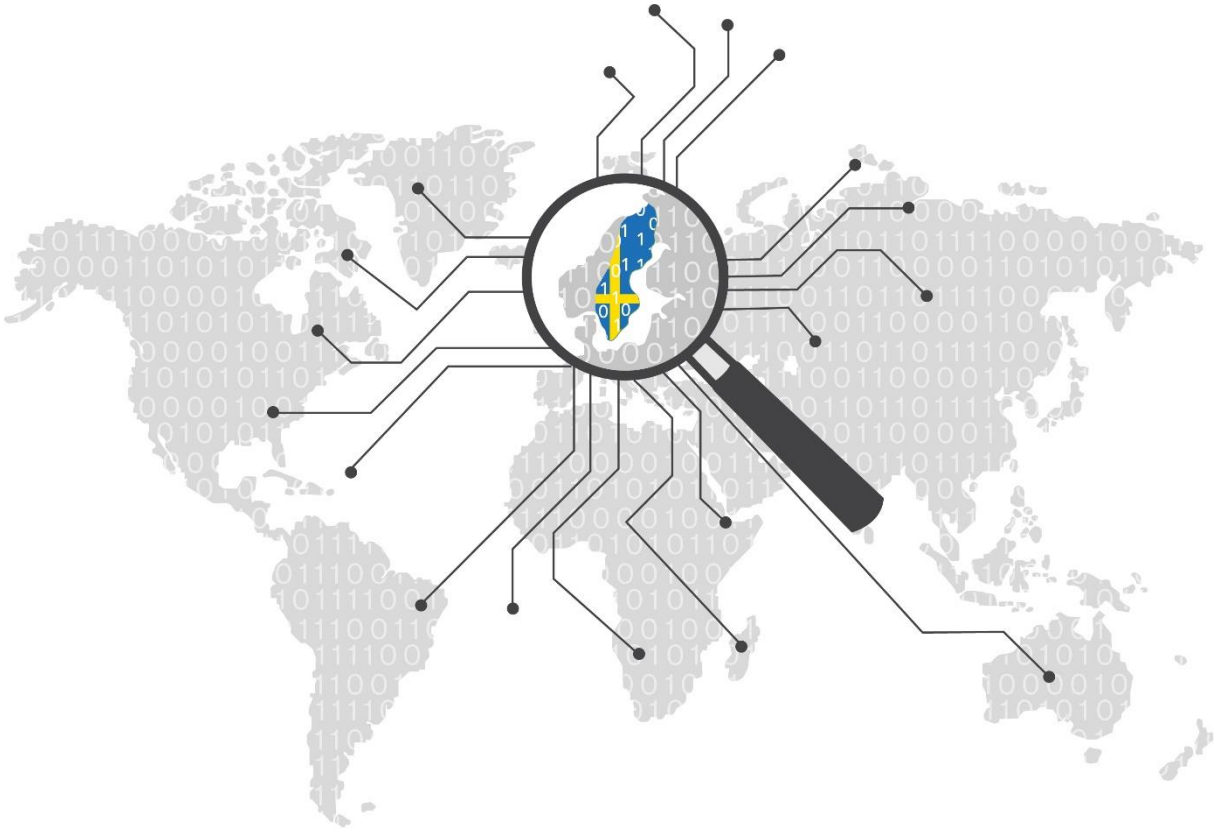


Vitbok

Molntjänster i samhällsbärande verksamhet – risker, lämplighet och vägen framåt

Försäkringskassan

Vitbok – Molntjänster i samhällsbärande verksamhet – risker, lämplighet och vägen framåt

Föräkringskassans diarienummer: 013428-2019

Version: 1.0

Datum: 2019-11-18

Försäkringskassan erbjuder som många andra myndigheter enklare tillgång till information och service samt effektiviserar interna processer med hjälp av digitala tjänster. Molntjänster erbjuder ofta god funktionalitet, driftsäkerhet och teknisk säkerhet till rimliga kostnader. Det är önskvärt och i viss utsträckning nödvändigt att den offentliga sektorn kan tillgodogöra sig dessa fördelar.

Samtidigt får vi aldrig bortse från den ökade sårbarhet som följer med digitaliseringen av samhällsbärande funktioner. Sveriges digitala suveränitet behöver säkras och den offentliga förvaltningen måste bibehålla eller ta tillbaka kontrollen över samhällsbärande digitala funktioner och data.

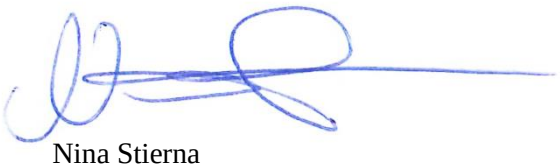
De beslut som fattas nu kommer sätta ramarna för vårt handlingsutrymme under överskådlig tid och påverka Sveriges förmåga att möta framtidens utmaningar. Valet av formen för it-drift i samhällsbärande verksamhet kommer att få konsekvenser för medborgarna, enskilda myndigheter och den samlade statsförvaltningen, men även för Sverige som stat.

Försäkringskassans allt ökande beroende av säkra, användarvänliga och robusta digitala tjänster innebär att myndigheten för egen del behöver klargöra om och när det är lämpligt och möjligt att använda publika molntjänster som erbjuds av privata leverantörer. Grunden för det ställningstagandet är vårt ansvar och vår skyldighet att hantera ofta mycket integritetskänsliga uppgifter om enskilda personer på ett så säkert sätt som möjligt. Även om analysen i denna vitbok utgår från Försäkringskassans verksamhet är vår förhoppning att den kan vara ett stöd även för andra som fattar strategiska beslut inom digitalisering och it.

Vitboken är beslutad av generaldirektör Nils Öberg, i närvaro av överdirektör Maria Rydbeck, IT-direktör Stefan Olowsson och rättschef Mikael Westberg, efter föredragning av den digitala strategen Anna Fors och den rättsliga experten Nina Stierna.

Nils Öberg
Generaldirektör

Anna Fors
Digital strateg



Nina Stierna
Rättslig expert

Innehåll

Sammanfattning

Försäkringskassan ser, som de flesta andra myndigheter, många fördelar med att använda digitala tjänster som tillhandahålls via Internet, så kallade molntjänster. Sådana tjänster har i många fall lett till ökad tillgänglighet och verksamhetsnytta samt god teknisk säkerhet till rimliga kostnader.

Flera stater, däribland USA, Kina och Indien, har numera lagstiftning som ger deras myndigheter rätt att under vissa förutsättningar ta del av data och uppgifter som lagras hos tjänsteleverantörer under sin jurisdiktion, även om lagringen sker utanför den egna statens territorium. Det har mot den bakgrunden uppstått en debatt om huruvida det är förenligt med svensk rätt och EU-rätt att använda sig av de molntjänster som erbjuds på marknaden. Försäkringskassan kan konstatera att det finns bestämmelser i såväl svensk rätt som EU-rätt som hindrar svenska myndigheter att använda vissa publika molntjänster i privat regi för att hantera sekretessreglerade uppgifter eller personuppgifter om leverantören träffas av sådan lagstiftning.

Vi anser emellertid att en helt central fråga i stort sett har förbigåtts i den svenska debatten, nämligen den som handlar om lämpligheten i att svenska myndigheter avhänder sig kontrollen över uppgifter i den verksamhet som vi benämner som samhällsbärande till privata företag eller andra länder. Till detta kommer olika säkerhetsrelaterade aspekter. Som exempel kan nämnas en ökad allmän sårbarhet, ökade risker för att obehöriga får tillgång till data samt svårigheter att säkerhetspröva personal och upprätta rättvisande risk- och sårbarhetsanalyser.

Försäkringskassan kommer inte att överlåta driften av digitala verksamhetskritiska system i samhällsbärande verksamhet till privata företag som står under jurisdiktion av en stat med sådan lagstiftning som nämnts ovan. För it-system i exempelvis säkerhetskänslig verksamhet kommer Försäkringskassans mål att vara it-drift i statlig regi.

För att säkra våra samhällsbärande funktioner mot cyberangrepp, värna den personliga integriteten och minska beroendet av enskilda tjänster på marknaden krävs därutöver att Sverige upprättar en myndighetsövergripande strategi och en långsiktig handlingsplan för digital suveränitet. För att svenska myndigheter ska kunna fortsätta att dra fördel av digitaliseringens alla möjligheter bör vi därutöver – genom samverkan nationellt och inom EU – se till att de privata tjänster vi väljer att använda anpassas till våra behov och gällande lagstiftning samt har en säkerhetsnivå som gör att vi kan behålla kontrollen över vår verksamhet och information. På så vis kan vi dra fördel av den innovationskraft och effektivitet som ofta är förknippad med privata it-tjänster, samtidigt som vi säkerställer Sveriges intresse av digital suveränitet.

Summary

Like many other governmental agencies, the Swedish Social Insurance Agency benefits from using so called cloud services. In many cases these services have led to better availability, operational benefits as well as a sound level of technical security at reasonable costs.

Several states, including the U.S., China and India, have legislation designed so that under specific circumstances their governmental agencies are given access to data and information stored by service providers under their jurisdiction, even if the physical storage is provided outside the territory of that state. With this in mind, a debate has risen on the compliance with Swedish and EU legislation when using a cloud service provided by the private market. The Swedish Social Insurance Agency notes that provisions in both Swedish and EU law prevents Swedish governmental agencies from using some public cloud services provided by private service providers, for the purpose of handling confidential information or personal data, if the service provider is under the jurisdiction of a state that has such legislation.

We are, however, of the opinion that an essential issue has not been addressed in the Swedish debate, namely whether it is suitable for Swedish governmental agencies to hand over to private companies or other countries control of information concerning activities we consider to be necessary for ensuring the crucial functions of our society. There are also a number of security related issues. For example, the possibility of increased general vulnerability, an increased risk of unauthorised access to data, as well as difficulties in conducting security checks of technical staff and accurate risk and vulnerability analysis.

The Swedish Social Insurance Agency will not contract the operation of critical digital systems in activities that are necessary for ensuring the crucial functions of our society to private companies under the jurisdiction of states with the type of legislation mentioned above. Regarding IT-systems in security sensitive activities, the objective of the Swedish Social Insurance Agency is for IT-systems to be under governmental auspices.

In order to ensure that functions crucial to society are secure against cyberattacks, to protect privacy and to reduce dependence on the provision of individual services by the private market, Sweden needs to formulate an overarching governmental strategy and a long-term action plan to protect digital sovereignty. In addition, in order for Swedish governmental agencies to continue to benefit from all the opportunities provided by digitalisation, we should ensure – through cooperation nationally and within the EU – that the private services we choose to use are adapted to our requirements and current legislation and have a level of security that allows us to maintain control of our activities and information. This will enable Sweden to take advantage of the innovation and efficiency often associated with IT-services provided by the private market whilst at the same time securing the digital sovereignty of Sweden.

Bakgrund

I regeringens digitala agenda för Sverige betonas vikten av att privata och offentliga aktörer agerar ansvarsfullt. Digitala system ska vara säkra och den personliga integriteten ska värnas. Regeringen framhåller även den ökade sårbarhet som följer av det ökade teknikberoendet samt att allmänhetens tillit är beroende av teknikens säkerhet.[1]

Molntjänster blir allt vanligare, även bland svenska myndigheter. I en undersökning som genomfördes 2018 uppgav en stor andel av Sveriges myndigheter att de använder minst en så kallad publik molntjänst som tillhandahålls av en privat leverantör.[2]

---

1 Näringsdepartementet, *Med medborgaren i centrum – Regeringens strategi för en digitalt samverkande statsförvaltning* (N2012:37)

2 Se bilaga 2 för definitioner av molntjänster samt beskrivning av molntjänsters användning. Se Bilaga 1 för en historisk återblick av outsourcing av statsförvaltningen samt Hellberg, Islam, Karlsson, *Säkerhet vid molnlösningar,* Örebro Universitet och Myndigheten för samhällsskydd och beredskap, s. 25.

Syfte

I detta dokument sammanställer vi inledningsvis fakta som har betydelse för Försäkringskassans användande av publika molntjänster som erbjuds av privata aktörer. Syftet med detta är främst att skapa underlag för ett välgrundat ställningstagande om Försäkringskassans möjligheter att använda dessa molntjänster vid genomförandet av sitt uppdrag. Vi har inte tagit ställning till de risker som finns med andra leveransmodeller och tekniker. Även om vitboken i den delen tar sikte på Försäkringskassans verksamhet är det vår förhoppning att vi genom detta arbete kan bistå med ett underlag för andra som bedriver det vi kallar samhällsbärande verksamhet. Vår förhoppning är också att detta dokument kan leda till att frågan om hur Sverige kan säkra kontrollen över it-tjänster i samhällsbärande verksamheter får en mer framträdande position än i dag.

Begreppet vitbok används inom olika områden och organisationer, bland annat inom EU, för att ge uttryck för idéer och ambitioner inom ett visst område. Begreppet passar således bra för det vi vill åstadkomma med detta arbete. Vi tar i detta dokument ställning i frågan om användning i Försäkringskassan av molntjänster som erbjuds av privata aktörer och önskar samtidigt att innehållet kan bidra till en fördjupad och breddad diskussion i en för hela samhället angelägen fråga. Våra slutsatser i detta dokument kommer att successivt arbetas in i våra interna administrativa styr- och stöddokument i de fall det är relevant.

I vår kartläggning och analys fokuserar vi på den verksamhet som vi kallar samhällsbärande. Detta begrepp är valt utifrån att vår analys pekar på ett behov av att säkra både samhällsviktig verksamhet och sådana funktioner som i sig inte omfattas av den definitionen, men som samhällsviktig verksamhet är beroende av. Genom att använda det bredare begreppet samhällsbärande verksamhet kan vi också vidga diskussionen och utgå från ett systemperspektiv på de funktioner som Sverige är beroende av för att fungera.

Molntjänster som leveransmodell

Molntjänst innebär att funktioner som annars skulle hanteras av egna datorer tillgängliggörs via Internet från leverantörens datorer eller servrar.[3] Detta kan innebära stora fördelar både för leverantörer och kunder. Tidigare genomförda utredningar pekar på stora nyttor för den offentliga sektorn om dessa tekniker kan användas för att möjliggöra en säker och kostnadseffektiv digitalisering av verksamheten.[4]

Molntjänster erbjuds i tre principiella former, om man utgår från förhållandet mellan kunden och leverantören:[5]

- *Publika molntjänster*, som innebär att en tjänst erbjuds till flera kunder som delar på samma infrastruktur, t.ex. servar. Kundernas datamängder hålls emellertid åtskilda, åtminstone virtuellt.

- *Partnermolntjänster*, som vänder sig till en specifik kundgrupp, till exempel myndigheter. Kunders datamängder kan hållas åtskilda åtminstone virtuellt, i det fall tjänsten förutsätter det.[6]

- *Privata molntjänster*, som leverantören bara erbjuder till en specifik kund.[7]

Dessa tre former av molntjänster kan erbjudas av antingen privata eller offentliga aktörer. Om en molntjänst är publik eller privat har således inte något att göra med vem som tillhandahåller tjänsten.

De utmaningar som är förknippade med molntjänsterna skiljer sig åt beroende på hur tjänsten är utformad tekniskt och avtalsmässigt. Det finns dock ett stort intresse i den svenska offentliga sektorn att använda de internationella publika molntjänster som erbjuds av privata företag.[8]

Mot den bakgrunden behandlar vi i denna vitbok främst de problem som kan uppstå när en myndighet använder sig av en publik molntjänst som tillhandahålls av privata leverantörer. Analysen kan dock i vissa delar vara applicerbar även på andra former av molntjänster eller för den delen andra former av it-tjänster.

---

[3] Ibland används begrepp som datormoln, molnet eller cloudtjänster.

[4] Pensionsmyndigheten, *Molntjänster i staten – en ny generation av outsourcing*, 2016 och Statens servicecenter, *En gemensam statlig molntjänst för myndigheternas it-drift* – Delrapport i regeringsuppdrag om samordning och omlokalisering av myndighetsfunktioner, (DNR 10052-2016/1121), 2017-02-07

[5] För mer utförlig beskrivning av molntjänster som leveransmodell, se bilaga 2.

[6] Vissa partnertjänster är uppbyggda för att de som ingår i samverkan ska kunna utbyta och dela information medan andra partnertjänster är uppbyggda precis som publika molntjänster med helt separata datamängder.

[7] De definitioner som används är de som använts i Pensionsmyndighetens utredning. Se Pensionsmyndigheten, *Molntjänster i staten*, s. 9. Se även vidare i bilaga 2.

[8] Se vidare bilaga 2.

Tredjeländers lagstiftning om tillgång till e-bevisning – exemplet USA

För att säkra tillgången till e-bevisning (det vill säga digitalt lagrad information, exempelvis mejl eller hur någon ringt, mejlat eller skickat sms) har vissa stater inrättat lagstiftning som ger en långtgående möjlighet att säkra sådan bevisning. Det mest omtalade exemplet är amerikanska Clarifying Lawful Overseas Use of Data Act (CLOUD Act).

För att illustrera hur sådan lagstiftning kan vara utformad och vilka rättsliga problem den kan föra med sig redogör vi i det följande för CLOUD Act och den debatt som förts kring denna lagstiftning. Det är emellertid viktigt att hålla i minnet att liknande lagstiftning även finns i flera andra länder, t.ex. Kina, Indien och Ryssland.[9]

CLOUD Act – en översikt

I detta avsnitt ger vi en översiktlig beskrivning av CLOUD Act, som trädde i kraft i mars 2018.[10] Denna lagstiftning ger amerikanska myndigheter möjlighet att begära att bl.a. leverantörer av elektroniska kommunikationstjänster och molntjänster (nedan tjänsteleverantörer) som är underkastade amerikansk jurisdiktion, bevarar eller lämnar ut data som är under leverantörens kontroll.[11]

Det spelar i sammanhanget inte någon roll om informationen lagras eller hanteras i eller utanför USA.[12] En sådan begäran ska – något förenklat – ske genom en s.k. ”warrant” som utfärdats av en domstol, ett administrativt föreläggande, ett föreläggande från en grand jury eller ett domstolsbeslut.[13]

---

9 Kammarkollegiet, *Förstudierapport Webbaserat kontorsstöd*, Dnr 23.2-6283-18, 2019-02-22, s. 24.

10 För en mer utförlig redogörelse, se t.ex. Council of Bars and Law Societies of Europe, *CCBE Assessment of the U.S. CLOUD Act*, 2019-02-28. Formellt utgör CLOUD Act ändringar och tillägg till United States Code och mer specifikt till den del som utgörs av the Stored Communication Act (SCA), som reglerar utlämnande av digital kommunikation som lagras hos leverantörer av elektroniska kommunikationstjänster m.fl. (18 U.S.C. Chapter 121 2701–2712). Bakgrunden till CLOUD Act var en tvist mellan Förenta staterna och Microsoft, som blev föremål för domstolsprövning genom målet United States v. Microsoft Corp., 584 U.S. (2018). Microsoft hade vägrat att lämna ut en privatpersons e-postmeddelanden, som lagrades på en server på Irland, till amerikanska Justitiedepartementet. Microsoft hävdade att dåvarande lagstiftning inte gav stöd för Justitiedepartementets krav på tillgång, eftersom informationen lagrades utanför USA. Innan USA:s högsta domstol avgjorde frågan undanröjdes den dock eftersom den amerikanska kongressen antog CLOUD Act. Om de begärda uppgifterna därefter lämnades ut i enlighet med CLOUD Act eller inte är oklart.

11 I 18 USC 2713 beskrivs de rättssubjekt som omfattas av bestämmelserna som “a provider of electronic communication service or remote computing service”. Det kan här vidare noteras att den amerikanska jurisdiktionen troligtvis är vidsträckt. Electronic Frontier Foundation menar att exempelvis den tyska meddelandetjänsten Telegram kan anses ligga under amerikansk jurisdiktion eftersom den erbjuder tjänster till amerikanska kunder. Se Electronic frontier Foundation, *The U.S. CLOUD Act and the EU: A Privacy Protection Race to the Bottom*, 2018-04-09.

12 18 USC 2713

13 18 USC 2703(b)(1)(A-B)

Tjänsteleverantören har möjlighet att bestrida myndigheternas begäran om tillgång till uppgifter i domstol om

- personen som uppgifterna rör inte är en ”United States Person”[14] och inte heller bor i USA,
- det finns en risk för att tjänsteleverantören genom att följa aktuell begäran skulle bryta mot en annan stats lagstiftning och
- den staten har ingått ett s.k. verkställighetsavtal (eng. executive agreement) med USA.[15]

Efter en sådan invändning ska domstol bedöma om dessa kriterier är uppfyllda samt utifrån samtliga omständigheter göra en avvägning mellan de intressen som talar för respektive emot ett utlämnande (eng. comity analysis).[16] Vid denna avvägning ska domstolen beakta bl.a.

- den amerikanska statens intressen,
- den andra statens intressen av att förhindra ett utlämnande som är förbjudet enligt den statens lag,
- risken för och omfattningen av de påföljder som kan drabba tjänsteleverantören vid ett utlämnande som strider mot lag i den andra staten, samt
- vilka kopplingar tjänsteleverantören och den person som informationen gäller har till USA.[17]

I vilken utsträckning en tjänsteleverantör kan bestrida en begäran enligt CLOUD Act om förutsättningarna ovan inte är uppfyllda är oklart.[18]

CLOUD Act ger också USA:s justitieminister möjlighet att genom ett sådant verkställighetsavtal med andra stater som nyss nämnts reglera möjligheten för dessa stater att direkt hos amerikanska tjänsteleverantörer begära information i syfte att bekämpa allvarlig brottslighet.[19] Justitieministern ska innan sådana avtal ingås bl.a. säkerställa att den andra statens lagstiftning ger ett tillräckligt skydd för integriteten och mänskliga rättigheter, både materiellt och processuellt.[20]

---

[14] United States Person är t.ex. den som är amerikansk medborgare eller som lagligen har rätt att vistas i USA, se 18 USC 2703 (h) med hänvisning till 2523 (a)(2).

[15] 18 USC 2703 (h) jämförd med 2523 (b) och (d). Notera att Sverige för närvarande inte ingått ett sådant avtal.

[16] 18 USC 2703 (h)(2)(B)

[17] 18 USC 2703 (h)(3)

[18] EPDB-EDPS, *Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection*, 2019-07-10, Annex s. 1–2

[19] Ett sådant avtal ingås av justitieministern (Attorney General) efter godkännande av utrikesministern (Secretary of State). Avtalet ska läggas fram till USA:s kongress, som har 180 dagar på sig att invända mot avtalet för att det inte ska träda i kraft. Se 18 USC 2523 (b) och (d).

[20] 18 USC 2523 (e). Ett sådant avtal ska ses över vart femte år.

Debatten kring CLOUD Act

Ur rättssäkerhetssynpunkt är det givetvis en fördel att förutsättningarna för amerikanska myndigheter att begära tillgång till data som lagras utanför USA nu regleras i lag.[21] De stora molntjänstleverantörerna har också gett uttryck för uppfattningen att CLOUD Act utgör en rimlig avvägning mellan individers rättigheter och brottsbekämpande myndigheters behov.[22] Det saknas dock inte kritiska röster; ett flertal amerikanska teknikföretag har uttryckt farhågor om att avsaknaden av en överenskommelse mellan USA och EU vad gäller brotts-bekämpande myndigheters tillgång till data riskerar amerikanska affärsintressen i Europa, bl.a. med hänsyn till potentiella lagkonflikter.[23]

Allvarlig kritik har också uttryckts vad gäller skyddet för mänskliga rättigheter. Europeiska advokatsamfundet menar att CLOUD Act inte tillgodoser den europeiska minimistandard som fastställts av Europadomstolen och EU-domstolen när det gäller staters elektroniska övervakning av medborgarna.

Flera fristående människorättsorganisationer pekar också på att skyddet för mänskliga rättigheter åsidosätts när amerikanska verkställande myndigheter ges möjlighet att ingå internationella avtal utan föregående granskning av kongressen. Dessa organisationer menar även att CLOUD Act öppnar för risken att avtal ingås med stater som är kända för att bryta mot mänskliga rättigheter. Därmed ökar också risken för att stater får tillgång till information som används för att kränka dessa rättigheter.[24]

Europeiska dataskyddsstyrelsen[25] och Europeiska datatillsynsmannen[26] har uppmärksammat att CLOUD Act även ger möjlighet att begära metadata från tjänste-leverantörerna. Dessutom påpekar dessa institutioner att en begäran enligt CLOUD Act inte alltid måste föregås av en domstolsprövning eller uppfylla krav på skälig misstanke. Så uppges exempelvis vara fallet när det gäller ett administrativt föreläggande eller ett föreläggande från en grand jury.[27] Om USA ingår avtal med ett tredjeland öppnas dessutom möjligheten för detta land att i realtid övervaka kommunikation som går via tjänsteleverantörerna.[28]

Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen uttrycker också farhågor vad gäller de möjligheter CLOUD Act ger för amerikanska myndigheter att

---

[21] Se exempelvis U.S Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, White Paper, april 2019, Microsoft, *Molntjänster och säkerhet* och Council of Bars and Law Societies of Europe, *CCBE Assessment*.

[22] Se exempelvis Punke Michael, *AWS and the CLOUD Act*, *AWS Security Blog*, 2019-05-27.

[23] ACT – The App Association m.fl, Öppet brev till Attorney General Barr, 2019-06-21

[24] Brev till amerikanska kongressen från 24 organisationer, däribland Amnesty International USA, Electronic Frontier Foundation och Human Rights Watch, 2018-03-12

[25] Europeiska dataskyddsstyrelsen (EDPB) är ett EU-organ, som bl.a. består av representanter från varje medlemsstats dataskyddsmyndighet. EDPB:s uppdrag är bl.a. att främja en konsekvent tillämpning av dataskyddslagstiftningen inom hela EU. Inom ramen för detta arbete utfärdar EDPB bl.a. riktlinjer för tolkning av grundläggande begrepp i GDPR.

[26] Europeiska datatillsynsmannen (EDPS) övervakar den behandling av personuppgifter som sker inom EU:s institutioner och organ. Genom att bl.a. ge råd, hantera klagomål och genomföra utredningar värnar EDPS den enskildes rätt till privatliv.

[27] Administrative subpoena eller grand jury subpoena.

[28] EPDB-EDPS, *Joint Response*, Annex s. 2 och 9

dela med sig av personuppgifter som erhållits med stöd av den lagen till andra tredjeländer.[29]

En begäran om tillgång till information som lagras i andra stater sker ofta genom instrument för ömsesidig rättslig hjälp, kallade *mutual legal assistance treaty* (MLAT). Det förfarande som då används kan vara långdraget, vilket ger stora utmaningar när det gäller att tillgodose det ökande behovet av e-bevisning i brottsutredningar. Vid tillämpning av CLOUD Act används i regel inte MLAT-förfarandet.[30]

Amerikanska justitiedepartementet har gett uttryck för att CLOUD Act är ett steg i rätt riktning för att komma till rätta med de svårigheter som finns vad gäller att få tillgång till avgörande digitala bevis som lagras i tredje länder.[31] MLAT-proceduren säkerställer dock att processuella och materiella regler i det land där informationen finns upprätthålls och att de rättsliga befogenheterna i detta land respekteras.[32]

I en resolution från Europaparlamentet uttrycks att en mer balanserad lösning jämfört med CLOUD Act hade varit att stärka befintliga internationella system för ömsesidig rättslig hjälp, i syfte att främja internationellt och rättsligt samarbete.[33] Samma uppfattning har förts fram av Europeiska Advokatsamfundet, som också menar att CLOUD Act undergräver den strävan som finns att anpassa det internationella samarbetet till de utmaningar brottsbekämpande myndigheter möter i det nya informationssamhället.[34]

---

[29] EPDB-EDPS, *Joint Response*, Annex s. 2 och 9

[30] U.S Departement of Justice, White Paper, april 2019

[31] U.S Departement of Justice, White paper och Jennifer Daskal, *Unpacking the CLOUD Act, EUCRIM*, 2019-01-31

[32] Se bl.a. Council of Bars and Law Societies of Europe, CCBE *Assessment* och Electronic Frontier Foundation, *EFF and 23 Groups Tell Congress to Oppose the CLOUD Act*, 2018-03-11. Se även Europeiska kommissionen, *Brief of the European Commission on behalf of the European Union as amicus curiae in support of neither Party in the case United States v. Microsoft Corp. No. 17-2*, s. 21 och EPDB-EDPS, *Joint Response*, Annex s. 3.

[33] Europaparlamentets resolution av den 5 juli 2018 om huruvida ett adekvat skydd säkerställs genom skölden för skydd av privatlivet i EU och USA (2018/2645(RSP)), s. 27 och 28

[34] Council of Bars and Law Societies of Europe, *CCBE Assessment*

Konflikter mellan CLOUD Act-liknande lagstiftning, EU-rätt och nationell rätt

Som tidigare nämnts är det inte bara USA som infört lagstiftning som ger landets myndigheter rätt att begära ut data, uppgifter och information som lagras i andra stater utan att internationell rättshjälp anlitas och utan att det krävs en bedömning enligt lagstiftningen i det land där uppgifterna lagras fysiskt. Eftersom de största och mest använda molntjänsterna på marknaden tillhandahålls av amerikanska bolag är det emellertid CLOUD Act som i praktiken, åtminstone hittills, varit av störst intresse. Utöver den debatt som tidigare nämnts har diskussionen gällt de konflikter som finns mellan CLOUD Act och annan liknande lagstiftning å ena sidan och EU-rätt respektive nationell rätt å andra sidan. I detta avsnitt sammanfattar vi kort dessa normkonflikter vad gäller områdena offentlighet och sekretess samt dataskydd.[35] En viktig principiell frågeställning är därutöver hur CLOUD Act och liknande lagstiftning förhåller sig till det mer övergripande skydd för den personliga integriteten som svenska myndigheter är skyldiga att upprätthålla enligt bl.a. grundlag och internationella konventioner.[36] Denna fråga behandlas emellertid inte i detta sammanhang.

Offentlighet och sekretess

Sekretess innebär ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt. Om det finns en bestämmelse om sekretess för en uppgift är uppgiften sekretessreglerad.[37]

Innan en svensk myndighet gör sekretessreglerade uppgifter tillgängliga för en tjänsteleverantör, måste myndigheten bl.a. analysera om detta innebär ett röjande av uppgifter i den mening som avses i offentlighets- och sekretesslagen (2009:400). eSamverkansprogrammets rättsliga expertgrupp (nedan eSam) gjorde 2018 ett rättsligt uttalande som tog sikte på röjandebegreppet vid användande av molntjänster som lyder under utländsk lagstiftning.[38] Detta uttalande kompletterades i september 2019. eSam anser att den svenska sekretesslagstiftningen innebär att en bedömning av om sekretessreglerade uppgifter ska anses röjda när de tillgängliggörs för en tjänsteleverantör ska göras i två steg.

Först ska en prövning göras om tjänsteleverantören enligt avtal med uppdragsgivaren inte får ta del av eller vidarebefordra de uppgifter som görs tekniskt tillgängliga för leverantören. Detta innebär att det ska finnas en juridiskt bindande och sanktionerad avtalssekretess för leverantören. Leverantören får inte heller vara bunden av regler i främmande rätt om att lämna ut uppgifter utan en föregående sekretessprövning eller annan laglig grund enligt svensk rätt för ett utlämnande. Om detta första villkor är uppfyllt, ska i *ett andra steg* en bedömning göras av om

---

[35] För en mer detaljerad redogörelse för dessa normkonflikter, se bilaga 3.

[36] Se 2 kap. 6 § samt målsättningsstadgandet i 1 kap. 2 § RF, artikel 8 i den europeiska konventionen den 4 november 1950 angående skydd för de mänskliga rättigheterna och de grundläggande friheterna och artikel 7 och 8 i EU:s stadga om de grundläggande rättigheterna.

[37] 3 kap. 1 § offentlighets- och sekretesslagen

[38] eSam är ett medlemsdrivet program för samverkan mellan 23 förvaltningsmyndigheter under regeringen och Sveriges kommuner och landsting, se www.esamverka.se.

omständigheterna i övrigt medför att det är osannolikt att tjänsteleverantören ändå tar del av eller vidarebefordrar uppgifterna.

Om det brister i någon av dessa två förutsättningar, ska de aktuella uppgifterna anses röjda direkt när de tillgängliggörs för tjänsteleverantören.[39] Om uppgifterna är sekretessbelagda krävs i så fall att den myndighet som röjer uppgifterna har stöd i lag eller förordning för att lämna ut dem.

Kammarkollegiet instämde 2019 i eSams bedömning.[40] Kammarkollegiet uttalade vidare att det inte är förenligt med offentlighets- och sekretesslagen att en tjänsteleverantör som anlitats av en svensk myndighet lämnar ut sekretessbelagda uppgifter till en utländsk myndighet i enlighet med CLOUD Act eller annan liknande lagstiftning. Detta beror – något förenklat – på att det inte finns någon särskild föreskrift i lag eller förordning som medger ett sådant utlämnande. Det är heller inte möjligt att säkerställa att en uppgift i motsvarande fall skulle ha fått lämnas ut till en svensk myndighet eller att säkerställa att svenska intressen tillgodoses.[41] Kammarkollegiet konstaterade också att en svensk myndighet som låter företag som lyder under ett regelverk liknande CLOUD Act hantera sekretessreglerade uppgifter, synes ge det utländska regelverket företräde framför svensk lagstiftning.[42]

En annan uppfattning har förts fram av marknadens aktörer, som hänvisar till det begränsade antalet ärenden enligt CLOUD Act som gällt utlämnande av uppgifter som lagras utanför USA:s gränser. Dessa aktörer menar även att en mer nyanserad bedömning måste göras av röjandebegreppet och att bl.a. kryptering och placering av serverhallar sätter problemet i ett annat ljus.[43] Sveriges kommuner och landsting (SKL) har, bl.a. med anledning av eSams ställningstagande, uttalat att molntjänster som erbjuds av den privata marknaden – även sådana med utländska ägarförhållanden – är en nödvändig del av digitaliseringen. SKL menar vidare att denna utveckling nu bromsas upp på grund av den osäkerhet som råder kring de rättsliga frågorna. SKL har också uttryckt farhågor gällande de investeringar som redan gjorts av en stor andel av Sveriges kommuner och regioner i publika molntjänster som erbjuds av den privata marknaden.[44] Vad gäller röjandebegreppet har SKL också uttalat att en dom från Arbetsdomstolen 2019 tyder på att uppgifter i sig inte ska anses röjda även om de lämnas ut till obehöriga i ett annat land.[45]

---

[39] eSamverkansprogrammet, *Rättsligt uttalande om röjande och molntjänster*, VER 2018:57, 2018-10-23 samt eSamverkansprogrammet, *Kompletterande information om molntjänster*, 2019-09-20

[40] Kammarkollegiet, *Förstudierapport Webbaserat kontorsstöd*, s. 35

[41] Jfr 8 kap. 3 § OSL

[42] Kammarkollegiet, Förstudierapport Webbaserat kontorsstöd, s. 32–33.

[43] Se bl.a. Microsoft, *Molntjänster och säkerhet*, Microsoft, Sveriges Kommuner och Landsting m.fl., Öppet seminarium på Almedalen 2019, *CLOUD Act – hinder eller ej* samt Fredrik Blix och Richard Brolin, *Grönt ljus för kommuner, regioner och statliga myndigheter att överväga molntjänster*, Cybercom Group, 2019-07-04.

[44] Sveriges Kommuner och Landsting, *Ställningstagande om informationshantering i vissa molntjänster*, ärendenr 19/00087, 2019-04-12

[45] Se Sveriges kommuner och Landsting, *Molntjänster och konfidentialitetsbedömning*, s.13. Det mål som avses är AD 2019 nr 15. Frågan i målet var om det funnits laga grund för avskedande av Transportstyrelsens f.d. generaldirektör. En av de frågor som behandlades var om staten förmått styrka att uppgifter om kvalificerade skyddsidentiteter blivit tillgängliga för två lagringstekniker (som förutsattes vara obehöriga) under sådana omständigheter att man måste räkna med att de skulle komma att ta del av uppgifterna och att generaldirektören således gjort sig skyldig till vårdslöshet med hemlig uppgift i enlighet med 19 kap. 9 § brottsbalken.

Dataskydd

Överföring till ett tredjeland av personuppgifter som lagras inom EU utgör en personuppgiftsbehandling. Under vilka förutsättningar en sådan behandling får ske regleras bl.a. 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 (allmän dataskyddsförordning), nedan kallad GDPR. Innan en svensk myndighet gör personuppgifter tillgängliga för en tjänsteleverantör, måste myndigheten således analysera om detta skulle innebära en risk för att uppgifterna behandlas i strid med GDPR.

Enligt Europeiska dataskyddsstyrelsens och Europeiska datatillsynsmannens bedömningar finns det enligt GDPR för närvarande endast i undantagsfall rättsliga förutsättningar för att föra över personuppgifter till ett tredjeland i enlighet med CLOUD Act. Det handlar om vissa exceptionella situationer där ett utlämnande av uppgifter krävs för att skydda den registrerades intressen. Europeiska dataskyddsstyrelsen har också framhållit att när det finns ett internationellt avtal om ömsesidig rättslig hjälp bör företag inom EU generellt avslå direkta förfrågningar och hänvisa tredjelandsmyndigheten till avtalet.[46]

En personuppgiftsansvarig eller ett personuppgiftsbiträde som i strid med GDPR lämnar ut personuppgifter till ett tredjelands myndigheter riskerar ytterst att drabbas av ansenliga administrativa sanktionsavgifter. Skulle en begäran enligt CLOUD Act inte hörsammas finns emellertid risk för rättsliga sanktioner i USA. I praktiken innebär detta att en tjänsteleverantör som anlitas av en svensk myndighet riskerar att utsättas för en konflikt mellan EU-rätten och amerikansk lagstiftning.[47]

En svensk myndighet är troligtvis inte personuppgiftsansvarig för den personuppgiftsbehandling som sker när ett anlitat personuppgiftsbiträde, t.ex. en tjänsteleverantör, lämnar ut uppgifter till ett tredjeland i strid mot avtalet.[48] Som personuppgiftsansvarig får myndigheten dock endast anlita biträden som ger tillräckliga garantier för att den registrerades rättigheter skyddas och för att behandlingen genomförs i enlighet med GDPR.[49] Den myndighet som vill använda sig av molntjänster måste därmed se till att inte anlita en tjänsteleverantör som kan komma att bryta mot GDPR eller mot personuppgiftsbiträdesavtalet.

---

[46] EPDB-EDPS, *Joint Response*, Annex s. 3. Se även Europeiska dataskyddsstyrelsen, *Riktlinjer 2/2018 för undantagen i artikel 49 enligt förordning 2016/679*, antagna den 25 maj 2018, s. 5.

[47] EPDB-EDPS, *Joint Response*, Annex s. 2

[48] Se vidare bilaga 3.

[49] Se artikel 28.1 i GDPR.

Samhällsbärande verksamhet

Som tidigare nämnts har vi i denna vitbok valt att utgå från det vi kallar samhällsbärande verksamhet. Enligt den avgränsning vi gjort utgörs en del av den verksamheten av samhällsviktig verksamhet, som är den man ofta talar om när det gäller myndigheterna. Samhällsviktig verksamhet definieras genom Myndigheten för samhällsskydd och beredskaps (MSB) föreskrifter. En liten del av den samhällsbärande verksamheten är dessutom s.k. säkerhetskänslig verksamhet. Denna definieras i säkerhetsskyddslagen (2018:585), där särskilda regler ställs upp till skydd för säkerhetskänslig information. I följande avsnitt redogör vi inledningsvis för begreppet samhällsviktig verksamhet. Utifrån det begreppet förklarar vi därefter vad vi innefattar i begreppet samhällsbärande verksamhet. Därpå följer en redogörelse för de risker som digitalisering av samhällsbärande verksamhet för med sig och en del av det skydd som finns för data och uppgifter som hanteras i samhällsbärande verksamhet.[50]

Vad är samhällsviktig verksamhet?

Totalförsvaret består av militärt respektive civilt försvar. Det civila försvaret utgörs av verksamhet som ansvariga aktörer genomför i syfte att göra det möjligt för samhället att hantera situationer då beredskapen höjs. Det civila försvaret bedrivs således i verksamhet hos statliga myndigheter, kommuner, regioner, privata företag och frivilligorganisationer. När det gäller det civila försvaret har Sverige tre mål, varav att säkerställa de viktigaste samhällsfunktionerna är ett.[51]

Samhällsviktig verksamhet är enligt MSB ett samlingsbegrepp som omfattar de verksamheter, anläggningar, noder, infrastrukturer och tjänster som är av avgörande betydelse för att upprätthålla viktiga samhällsfunktioner inom en samhällssektor. Dessa verksamheter bedrivs av ett stort antal privata och offentliga aktörer.[52] Samhällsviktig verksamhet innefattar sammanfattningsvis sådan verksamhet som vid störningar i eller bortfall av verksamheten kan orsaka kriser som hotar samhället. Det kan även handla om en verksamhet som behövs för att hantera en potentiell eller pågående kris.[53] MSB har identifierat elva sektorer där samhällsviktig verksamhet bedrivs för att upprätthålla viktiga samhällsfunktioner. Bland dessa återfinns en bred samling av sektorer, bl.a. energiförsörjning, hälso- och sjukvård, omsorg och

---

[50] Data definieras enligt ISO/IEC 2382:2015 som en representation av information som kan tolkas efter upprättande och som återfinns i en form så det kan kommuniceras, tolkas eller processas. Information definieras enligt samma standard som kunskap om objekt, till exempel fakta om händelser, saker, processer eller idéer. Information ska alltid ses inom sin kontext. Se International Organization for Standardization, *ISO/IEC 2382:2015(en)Information technology — Vocabulary.*

[51] Prop. 2014/15:109, *Försvarspolitisk inriktning – Sveriges försvar 2016-2020,* s. 12. Försvarsutskottets betänkande 2014/15:FöU11 och Riksdagens protokoll 2014/15:117.

[52] Myndigheten för samhällsskydd och beredskap, *Vägledning för identifiering av samhällsviktig verksamhet*, MSB1408, juni 2019, s. 7

[53] Se Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters risk- och sårbarhetsanalyser (MSB 2016:7) 2 §. Här definieras samhällsviktig verksamhet som en verksamhet som uppfyller minst ett av två villkor. 1) Ett bortfall av eller en svår störning i verksamheten kan ensamt eller tillsammans med motsvarande händelser i andra verksamheter på kort tid leda till att en allvarlig kris inträffar i samhället. 2) Verksamheten är nödvändig eller mycket väsentlig för att en redan inträffad kris i samhället ska kunna hanteras så att skadeverkningarna blir så små som möjligt.

transporter. Andra exempel är kommunalteknisk försörjning, som innefattar de viktiga funktionerna dricksvattenförsörjning, avloppshantering, renhållning och väghållning samt socialförsäkringar, där det allmänna pensionssystemet samt sjuk- och arbetslöshetsförsäkringarna ingår.[54]

Vad innefattar vi i samhällsbärande verksamhet?

Som framgår ovan innefattar begreppet samhällsviktig verksamhet verksamheter som är avgörande för att viktiga funktioner i samhället ska fungera. För att detta ska ske i praktiken krävs emellertid ofta kontinuitet i funktioner och it-system som inte i sig kategoriseras som samhällsviktiga. Som exempel kan nämnas att samhällsviktiga funktioner som brandförsvar och sjukvård är beroende av något så enkelt som att barnomsorgen för dess personal fungerar. Vi har i denna vitbok valt att använda begreppet samhällsbärande verksamhet för att beskriva både de verksamheter som är samhällsviktiga och de verksamheter som samhällsviktig verksamhet på något sätt är beroende av för att fungera. Vår definition av samhällsbärande verksamhet utgår således ifrån MSB:s definition av samhällsviktig verksamhet. Gränsen för vad som ska ses som samhällsbärande verksamhet är emellertid inte enkel att fastställa. Samhället utvecklas kontinuerligt och beroenden mellan verksamheter förändras. Det krävs således att varje myndighet som bedriver samhällsviktig verksamhet identifierar vilka andra funktioner denna verksamhet är beroende av för att fungera.

Utöver den samhällsbärande och samhällsviktiga verksamheten finns ytterligare en nivå av verksamhet, nämligen den säkerhetskänsliga, som bl.a. innefattar verksamhet som är av betydelse för Sveriges säkerhet. Mer om sådan verksamhet finns att läsa nedan under rubriken *Säkerhetsskyddet*. Med en schematisk skiss kan förhållandet mellan de olika typerna av verksamhet åskådliggöras på följande sätt.

Illustration av förhållandet mellan begreppen samhällsbärande, samhällsviktig och säkerhetskänslig. En del av den samhällsbärande verksamheten utgörs av samhällsviktig verksamhet, som i sin tur till viss del består av säkerhetskänslig verksamhet.

[54] MSB, *Vägledning för identifiering av samhällsviktig verksamhet*, s. 7

Identifierade risker till följd av digitalisering och utkontraktering av samhällsbärande verksamheter

Som en följd av bl.a. teknik- och tjänsteutveckling, privatisering, utkontraktering och automatisering går utvecklingen i samhället mot fler och mer komplexa beroenden mellan olika verksamheter. MSB har konstaterat är det viktigt att teknikutvecklingen inte påverkar samhällets förmåga att motstå och hantera störningar.[55]

Säkerhetspolisen har identifierat teknikutvecklingen som ett av sju hot mot Sverige under 2019.[56] Regeringen har också konstaterat att sårbarheten i dagens globala it-system är en av våra mest komplexa utmaningar och att den kommer att fortsätta att vara det under överskådlig tid. Operationer i cybermiljön har utvecklats till att utgöra ett separat hot, såväl som ett av flera militära maktmedel.[57] Antagonistiska it-angrepp från statliga eller statsstödda aktörer kan riktas mot vitala delar av samhället och få spridningseffekter till samhällsviktig verksamhet i flera sektorer.[58] Försvarsberedningen konstaterar att det militära försvaret är beroende av att det övriga samhällets grundläggande funktioner fortsätter att fungera före och under ett väpnat angrepp. Det blir därför allt svårare att säga var den civila infrastrukturen slutar och var den militära börjar.[59] För att upprätthålla en hög nivå av cybersäkerhet i Sverige menar regeringen att samhällsviktiga funktioner och it-system måste kunna skyddas mot it-angrepp. En del av Sveriges beslutade försvarspolitiska inriktning innebär att Sverige ska utveckla och förstärka sin samlade förmåga att förebygga, motverka och aktivt hantera konsekvenserna av civila och militära hot, händelser, attacker och angrepp i cybermiljön.[60]

I detta sammanhang bör också den underrättelseverksamhet som bedrivs av amerikanska myndigheter med stöd av the Foreign Intelligence Surveillance Act (FISA) nämnas. Genom systemet PRISM analyseras data som hämtats in från tjänsteleverantörer för underrättelseverksamhet riktad mot andra än amerikanska medborgare.[61] År 2013 avslöjades att miljontals användarkonton hos bl.a. Google omfattats av denna övervakning och att även metadata samlats in.[62] FISA gäller fortfarande men det är oklart hur den nu tillämpas och därmed vilken data som hämtas in med stöd av lagen.[63]

Säkerhetspolisen har identifierat utkontraktering av it, där molntjänster som tillhandahålls av privata aktörer ingår, som en potentiell risk. Säkerhetspolisen pekar

---

55 MSB, *Övergripande inriktning för samhällsskydd och beredskap*, s. 7

56 Säkerhetspolisen, *Årsbok 2018*, s. 21

57 Försvarets radioanstalt (FRA) menar att statliga cyberangrepp ständigt pågår och ökar fortlöpande. Syftet med dessa angrepp anges vara att komma över information, t.ex. om strategierna bakom Sveriges utrikespolitik, vårt samhälles sårbarheter eller Sveriges totalförsvar. Det kan också handla om förberedelser för senare angrepp och störningar eller industrispionage. Se Försvarets radioanstalt, *Årsrapport 2018*, s. 17 och 19.

58 Se prop. 2014/15:109, s. 111–113.

59 Ds 2017:66, *Motståndskraft – Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025*, s. 17 ff och s. 113

60 Se prop. 2014/15:109, s. 111–113.

61 Director of National Intelligence, *Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 2013-06-08

62 Gellman Barton and Soltani Ashkan, *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say*, The Washington Post, 2013-10-30

63 Europaparlamentet, *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*, (PE 583.137), s.127–128

på att detta ofta innebär att leverantören placerar olika kunders system och information i samma fysiska datorsystem. Detta medför en ökad risk eftersom en störning i en kunds system kan orsaka störningar eller avbrott i flera andra kunders system. Hamnar en stor mängd hemlig information hos en enskild leverantör riskerar denne dessutom att bli ett attraktivt mål för bland annat andra länders underrättelseinhämtning. Den mängd information som samlas hos en leverantör kan vidare medföra att leverantörens verksamhet sammantaget är av stor betydelse för Sveriges säkerhet.[64]

När det gäller specifikt molntjänster pekade Integritetskommittén på att det för myndigheter sammantaget finns allvarliga integritetsrisker med molntjänster, i synnerhet de publika. Anledningen till detta uppgavs bl.a. vara det stora antalet personuppgifter som myndigheter behandlar, vilka dessutom kan vara integritetskänsliga. Det handlar också om att myndigheter har en mängd regelverk att följa, t.ex. vad gäller allmänna handlingar, sekretess, arkivering och säkerhetsskydd. Det är enligt kommittén inte heller ovanligt att myndigheter köper molntjänster utan att skaffa sig närmare kunskaper om hur uppgifterna hanteras och sprids inom tjänsten. Små myndigheter kan också sakna kompetens att välja rätt slags molntjänst utifrån rättsliga och säkerhetsmässiga förutsättningar. Även myndigheters behandling av personuppgifter såsom arbetsgivare medför enligt Integritetskommittén risker när den sker i molntjänster. Att uppgifterna i allt större utsträckning hamnar hos externa leverantörer kan innebära en omfattande och svårkontrollerad spridning, lagring och vidareanvändning av uppgifterna. Flera led i den hanteringen görs många gånger utan vare sig arbetsgivarens eller arbetstagarnas kännedom.[65]

Ytterligare en riskfaktor när det gäller utkontraktering är tjänsteleverantörernas hantering av telemetridata. Telemetridata är mätdata som hämtas och hanteras av leverantören och som kan omfatta både faktiskt innehåll och metadata. Sådan data kan teoretiskt bli föremål för utlämnande i enlighet med lagstiftning som CLOUD Act, men hanteras främst av leverantören i syfte att förbättra och underhålla tjänsten. Intressant i detta sammanhang är att molntjänst som affärsmodell i sig ofta rymmer en inneboende drivkraft att använda kundernas uppgifter för egna ändamål, t.ex. för att utveckla nya tjänster, och att dela med sig av uppgifterna till andra företag, t.ex. som annonsunderlag.[66] Även om vissa inställningar kan begränsa mängden telemetridata som hanteras av tjänsteleverantören kan kunderna inte styra detta helt. Standardavtal för molntjänster ger ofta leverantören goda möjligheter att hantera uppgifter för egna ändamål, även om sådana avtal strider mot dataskyddsregleringen. I en utredning genomförd av nederländska myndigheter konstateras att leverantörer av bland annat publika molntjänster utan lagligt stöd hämtar in potentiellt känsliga data (även metadata) och att de lämnar ut telemetridata till länder utanför EU.[67]

---

[64] Se bl.a. Säkerhetspolisen, *Årsbok 2017*, s. 56.

[65] Kommittén konstaterar också att den enskilde ofta inte har någon laglig möjlighet att motsätta sig att personuppgifter behandlas av myndigheter, vilket kan få långtgående effekter vid användning av molntjänster, eftersom uppgifter från förvaltningssfären då når privat sektor. Se Integritetskommittén, *Hur står det till med den personliga integriteten? – en kartläggning av Integritetskommittén* (SOU 2016:41) s. 53–54, 70 och 81.

[66] SOU 2016:41 s. 111

[67] Se bilaga 8 för mer detaljer avseende exempel på telemetridata som hanteras av leverantörer. Se även SOU 2016:41 s. 112.

Integritetskommittén konstaterade att de största riskerna för den personliga integriteten när det gäller molntjänster hänger ihop med den förlust av insyn och kontroll som användning av sådana tjänster i regel innebär. Utöver de risker som redan nämnts ovan kan sägas att denna förlust medför risker för obehörig åtkomst hos leverantörer och underleverantörer och för att uppgifterna hamnar i länder där lagstiftningen ger ett otillräckligt skydd. Uppgifterna riskerar också att hamna hos underleverantörer som är okända för kunden, vilket i sin tur kan göra det svårt för en personuppgiftsansvarig att uppfylla sin skyldighet att se till att uppgifterna hanteras i enlighet med dataskyddsregleringen.[68]

Säkerhetspolisen konstaterar vidare att allt fler myndigheter utkontrakterar särskilt skyddsvärda delar av sin verksamhet till leverantörer i andra länder, så kallad offshoring.[69] Myndigheterna har i dessa fall samma skyldighet att ställa krav på säkerhetsskyddsåtgärder som om leverantören vore baserad i Sverige. MSB konstaterar också att offshoring kräver särskilda hänsyn i arbetet med skydd för samhällsviktig verksamhet. Vid utkontraktering av verksamhet till en leverantör i ett annat land ska det därutöver i regel alltid finnas ett bilateralt säkerhetsskyddsavtal mellan Sverige och det land där leverantören har sitt säte.[70]

I en utredning avseende utkontrakteringen av Transportstyrelsens it-drift 2017 konstaterades att det innebär vissa risker att låta centrala delar av de tekniska system som får en svensk myndighet att överhuvudtaget fungera styras och underhållas av företag i andra länder. Utredaren drog slutsatsen att även system som ska vara öppna och tillgängliga och inte i sig innehåller känslig information kan vara av sådan samhällsbetydelse att det inte är lämpligt att kontrollen över dessa ligger någon annanstans än i Sverige.[71]

Skyddet för samhällsbärande verksamhet

I detta avsnitt gör vi ett nedslag i de regelverk som ställer upp ett skydd för myndigheternas verksamhet, med speciellt fokus på it-stöd. Vi behandlar även kryptering, som i vissa sammanhang har lyfts som en möjlig åtgärd för att hantera bl.a. de lagkonflikter som vi tidigare redogjort för.

De angivna områdena ska endast ses som exempel. Man måste således hålla i minnet att det därutöver även finns annan reglering. Som exempel kan nämnas lagstiftning som skyddar olika typer av uppgifter, som dataskydds- och sekretessregleringen.

---

[68] SOU 2016:41 s. 111

[69] Om den leverantör som erbjuder molntjänsten lagrar kunders data eller har teknisk personal i ett annat land betraktas detta som en form av offshoring.

[70] Säkerhetspolisen, *Årsbok 2017*, s. 56 och Myndigheten för samhällsskydd och beredskap, *Handlingsplan för skydd av samhällsviktig verksamhet,* MSB597, *dec 2013*, s. 17

[71] SOU 2018:6, Granskning av Transportstyrelsens upphandling av it-drift, s. 238

Risk- och sårbarhetsanalyser

Kommuner, regioner och det stora flertalet statliga myndigheter ska analysera om det finns sådan sårbarhet eller sådana hot och risker inom myndighetens ansvarsområde som synnerligen allvarligt kan försämra förmågan till verksamhet inom området (risk- och sårbarhetsanalys).

En sådan analys är ett första steg i en kedja för identifiera och reducera de sårbarheter, hot och risker som finns inom myndighetens ansvarsområde som synnerligen allvarligt kan försämra förmågan till verksamhet inom området.[72] När riskerna identifierats används analysen för att bedöma om en risknivå är acceptabel och – om så inte är fallet – vilka åtgärder som kan vidtas för att motverka uppkomsten eller minimera effekten av de identifierade riskerna.[73] MSB betonar att krisberedskapen måste säkerställas även vid upphandling av samhällsviktiga funktioner.[74]

Informationssäkerhet och informationsklassning

Samtliga statliga myndigheter under regeringen ska se till att de egna informationshanteringssystemen uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt.[75] Myndigheternas informationssäkerhetsarbete syftar till att bevara konfidentialitet, riktighet, spårbarhet och tillgänglighet hos information. För att åstadkomma detta ska en informationsklassning göras.

I denna identifieras skyddsbehovet för en viss informationstillgång. Detta sker genom att information klassas i olika nivåer utifrån vilka konsekvenser som kan uppstå av ett bristande skydd vad gäller konfidentialitet, riktighet och tillgänglighet.

Utifrån informationsklassningens resultat och genomförd riskanalys ska myndigheten sedan identifiera och vidta de åtgärder som krävs för att uppfylla skyddsbehovet. Vilken modell som ska tillämpas för arbetet beslutas av varje enskild myndighet.[76]

---

[72] Lagen (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap 2 kap. 1 § samt förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap 8 § och 16 § 2

[73] Myndigheten för samhällsskydd och beredskap, *Vägledning för risk- och sårbarhetsanalyser*, MSB245, april 2011, s. 50–51

[74] Myndigheten för samhällsskydd och beredskap, *Upphandling till samhällsviktig verksamhet – en vägledning*, MSB1275, september 2018, s. 19

[75] Se 3 och 19 §§ förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.

[76] 4 och 9 §§ Myndigheten för samhällsskydd och beredskap Föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1)

Säkerhetsskyddet

Som nämnts tidigare utgörs delar av det vi kallar samhällsbärande verksamhet av s.k. säkerhetskänslig verksamhet, vilken bl.a. innefattar verksamhet som är av betydelse för Sveriges säkerhet. Hur sådan verksamhet förebyggande ska skyddas mot spionerі, sabotage, terroristbrott och vissa andra hot regleras i säkerhetsskyddslagen.[77]

Säkerhetskänsliga verksamheter klassificeras utifrån vilken skada som uppstår för Sveriges säkerhet om en angripare inhämtar information om verksamheten, förstör information eller på annat sätt hindrar att verksamheten kan bedrivas.[78] Kraven på hanteringen av säkerhetsskyddsklassificerade uppgifter ökar med klassificeringsnivån. Säkerhetskänslig verksamhet bedrivs bl.a. av svenska myndigheter, t.ex. Försäkringskassan.

I säkerhetsskyddslagen finns bestämmelser om bl.a. informations- och personalsäkerhet. Informationssäkerhet handlar om att skydda information, oavsett var den finns, på ett sätt så att den inte kan delas med eller ändras av obehöriga personer. Det handlar också om att se till att information finns till hands när den behövs.[79]

När det gäller personalsäkerhet placeras en anställning eller annat deltagande i säkerhetskänslig verksamhet vanligen i säkerhetsklass, utifrån vilken typ av uppgifter personen kommer att få del av och i vilken utsträckning detta kommer att ske.[80] Den som ska anställa eller anlita en person i säkerhetskänslig verksamhet ska dessförinnan göra en säkerhetsprövning, som bl.a. ska visa om personen kan antas vara lojal med de intressen som ska skyddas och i övrigt pålitlig ur säkerhetssynpunkt.[81] I säkerhetsprövningen ingår en grundutredning, som kan innefatta bl.a. en intervju och inhämtning av relevanta intyg och referenser.[82] Grundutredningen följs av en registerkontroll, som utförs av Säkerhetspolisen.[83] Denna omfattar uppgifter som hämtas från belastningsregistret, misstankeregistret samt uppgifter som behandlas med stöd av lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område.[84] Svenskt medborgarskap är inte ett krav för personer som på ett annat sätt än genom anställning deltar i säkerhetskänslig verksamhet som bedrivs av stat, kommun eller region.[85] Om den person som ska anställas eller anlitas har eller har haft hemvist i ett annat land är Säkerhetspolisens möjligheter att genomföra kvalitativa registerkontroller dock begränsade. Säkerhetspolisen menar att verksamhetsutövaren i dessa fall måste ta höjd för detta, t.ex. genom att fördjupa bakgrundskontrollen och ställa högre krav på inhämtning av

---

77 1 kap. 1–2 §§ säkerhetsskyddslagen

78 2 kap. 5 § säkerhetsskyddslagen. De fyra säkerhetsskyddsklasserna är 1) kvalificerat hemlig om den skada som kan uppstå är synnerligen allvarlig, 2) hemlig vid en allvarlig skada, 3) konfidentiell vid en inte obetydlig skada och 4) begränsat hemlig vid endast ringa skada.

79 2 kap. 2 § säkerhetsskyddslagen. Se även Säkerhetspolisen, *Informationssäkerhet.*

80 3 kap. 5–10 §§ säkerhetsskyddslagen

81 2 kap. 4 § och 3 kap. 1–2 §§ säkerhetsskyddslagen. Se även Säkerhetspolisen, *Personalsäkerhet*.

82 3 kap. 3 och 4 §§ säkerhetsskyddslagen (2018:585), 5 kap. 2 § säkerhetsskyddsförordningen (2018:658) och 6 kap. 4 § Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd. Se även Säkerhetspolisen, *Vägledning i säkerhetsskydd*, s. 11–12

83 3 kap. 14 § säkerhetsskyddslagen (2018:585)

84 3 kap. 13 § säkerhetsskyddslagen

85 3 kap. 11 § säkerhetsskyddslagen

referenser.[86] Ett exempel på de svårigheter som finns när det gäller att säkerhetspröva utländska medborgare framgår av den utredning som genomfördes 2018 gällande Transportstyrelsens upphandling av it-drift.[87]

Om en myndighets säkerhetskänsliga verksamhet ska bedrivas av upphandlade leverantörer måste myndigheten kräva samma nivå på säkerhetsskyddet som skulle ställts inom den egna verksamheten.[88] Detta sker genom ett säkerhetsskyddsavtal, som tecknas med anbudsgivare, leverantörer och eventuella underleverantörer. Myndigheten ska också kontrollera och följa upp att leverantörerna faktiskt vidtagit de åtgärder som myndigheten ställt krav på genom säkerhetsskyddsavtalet.[89] En av riskerna vid upphandling i säkerhetskänslig verksamhet är enligt Säkerhetspolisen att de krav som ställs i säkerhetsskyddsavtalet ibland är så allmänt hållna att de är svåra att följa upp.[90]

Kryptering av data

Alla verksamhetsutövare – offentliga och privata – ska när säkerhetsskydds-klassificerade uppgifter kommuniceras till ett informationssystem utanför verksamhetsutövarens kontroll skydda uppgifterna med hjälp av kryptografiska funktioner som har godkänts av Försvarsmakten.[91] Många molntjänstleverantörer erbjuder sina kunder krypteringstjänster även för funktioner och verksamhet som inte omfattas av säkerhetsskyddsförordningen. Det har i vissa sammanhang framförts att eventuella problem relaterade till t.ex. tredjelands myndigheters åtkomst till data som lagras i molntjänster kan avhjälpas med sådana tjänster. [92]

Kryptering syftar förvisso till att obehöriga inte ska få tillgång till data. Om tjänsten är utformad så att en part, t.ex. tjänsteleverantören, kan anses vara behörig och därmed får tillgång till krypteringsnyckeln, skyddar krypteringen inte mot den partens tillgång. Kryptering får i regel en negativ inverkan på prestanda om åtkomsten till data begränsas för leverantören. Krypterade data kan inte heller bearbetas vilket innebär att möjliga användningsområden för många tjänster blir kraftigt begränsade.[93] Kammarkollegiet konstaterade bl.a. i sin förstudie avseende webbaserat kontorsstöd att kryptering inte är en realistisk skyddsåtgärd för kontorsapplikationer.[94]

---

[86] Säkerhetspolisen, *Vägledning i säkerhetsskydd*, s. 26

[87] Se SOU 2018:6, s.161–163.

[88] Säkerhetspolisen, Säkerhetsskydd vid upphandlingar och affärsavtal

[89] 2 kap. 6 § säkerhetsskyddslagen. Bestämmelsen avser upphandlingar och avtal om varor, tjänster eller byggentreprenader om det i upphandlingen förekommer säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre, eller om upphandlingen i övrigt avser eller ger leverantören tillgång till säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet.

[90] Säkerhetspolisen, *Årsbok 2017*, s. 56

[91] 3 kap 5 § säkerhetsskyddsförordningen (2018:658)

[92] Se vidare om kryptering i bilaga 7.

[93] Bearbetning är i praktiken alla åtgärder som vidtas för att data ska kunna hanteras på annat sätt än att lagras eller skickas. Om uppgifterna ska läsas eller redigeras innebär det bearbetning. Man kan likna krypterade data med brev i ett förslutet kuvert, där det förslutna kuvertet utgör krypteringen. Detta kuvert kan förvaras och förflyttas men för att någon ska kunna ta del av innehållet behöver kuvertet öppnas, vilket motsvarar att data dekrypteras. Se vidare bilaga 7.

[94] Kammarkollegiet, *Förstudierapport Webbaserat kontorsstöd*, s. 35. I den analys av Microsofts användning av telemetridata som nederländska myndigheter genomförde 2017, nämns kryptering inte heller som ett sätt att avhjälpa problemet med att tjänsteleverantörer tar del av känsliga data från sina kunder, se vidare bilaga 8.

Digital suveränitet

Sveriges säkerhetspolitik syftar ytterst till att garantera landets oberoende och självständighet. Det handlar om att värna vår suveränitet, svenska rättigheter och intressen och våra grundläggande värderingar samt om att skydda svensk handlingsfrihet inför politisk, militär eller annan påtryckning. Regeringen har gett uttryck för att en nödvändig förutsättning för att Sverige ska uppnå målen för vår säkerhet är att vi hävdar vårt lands suveränitet och territoriella integritet.[95]

Nationell suveränitet definieras som kontroll över nationens territorium, nationell kontroll över de politiska beslutsprocesserna i landet samt säkrande av nationens försörjning med förnödenheter. Nationell suveränitet kan ses som en förutsättning för att kunna värna övriga värden, som människors liv och hälsa, samhällets funktionalitet samt demokrati och rättssäkerhet.[96]

I en tid där samhällsbärande funktioner i allt större utsträckning är beroende av digitala system, får kontrollen över information i sådan verksamhet allt större betydelse för vårt lands möjlighet till oberoende. Försvarsberedningen lyfter fram att en utvecklad förmåga på informations- och cybersäkerhetsområdet ökar möjligheten att upprätthålla vår nationella suveränitet, aktivt bidra till att hantera händelser i närområdet och skydda kritisk infrastruktur.[97]

Begreppet digital suveränitet nämndes första gången i början av 2000-talet. Innebörden av begreppet tycks inledningsvis ha diskuterats bl.a. i Frankrike.[98] Diskussionerna tog dock fart 2013, i samband med att det avslöjades att vissa nationer bedrivit omfattande digital massövervakning av bland annat europeiska medborgare.[99] Bland de åtgärder som då diskuterades fanns en nationell meddelandetjänst (Tyskland), egna undervattenskablar för internettrafik (Finland och EU), lokala molntjänster för lagring (Frankrike, Tyskland, Schweiz och Polen) och nätverk för att säkra att datatrafik inte lämnade EU (Tyskland).[100]

Frankrike och Tyskland tillkännagav 2015 att länderna gemensamt kommer att driva frågan kring digital suveränitet på EU-nivå. Med detta avsågs att förstärka medlemsstaternas och EU:s kapacitet att skydda digitala nätverk, att utveckla en autonom, innovativ, effektiv och diversifierad digital industri särskilt avseende cybersäkerhet och betrodda tjänster i Europa samt att Europa självständigt ska kunna

---

95 Prop. 2014/15:109 s. 7

96 Se bl.a. MSB, *Övergripande inriktning för samhällsskydd och beredskap*, s. 7–8.

97 Ds 2017:66, s. 115

98 Bellanger Pierre, *De la souveraineté en général et de la souveraineté numérique en particulier*, *Les Échos*, 2011-08-30. Inledningsvis användes även begreppet teknisk suveränitet, se Maurer Tim m.fl., *Technological Sovereignty: Missing the Point? An Analysis of European Proposals after June* 5, 2013, New America's Open Technology Institute och the Global Public Policy Institute (GPPi), s. 4.

99 Tim Maurer m.fl., *Technological Sovereignty*, s. 3. Övervakningen reglerades i amerikanska Executive order 12333: Office of the Director of National Intelligence *United States Intelligence Activities (Federal Register Vol. 40, No. 235 (December 8, 1981), amended by EO 13284 (2003), EO 13355 (2004), and EO 13470 (2008)).*

100 Tim Maurer m.fl., *Technological Sovereignty*, s. 11

besluta om säkerhetsnivå för egna data.[101] Därutöver har digital suveränitet på EU-nivå nämnts vid ytterligare några tillfällen. Europeiska rådet menar att det behöver säkerställas att Europa har digital suveränitet och får sin rättmätiga andel av fördelarna med den digitala omvandlingen.[102]

I Europeiska unionens råds slutsatser om framtiden för ett starkt digitaliserat Europa efter 2020 understryks att Europas förmåga till cybersäkerhet måste stärkas, bl.a. för att skydda Europas digitala suveränitet.[103] Frågan om EU-ländernas suveränitet på viktiga teknikområden har också identifierats av EU-kommissionens tillträdande ordförande Ursula von der Leyen som en av åtgärderna för att rusta Europa för den digitala tidsåldern.[104] Representanter för Europeiska datatillsynsmannen har också berört frågan om digital suveränitet, genom att ge uttryck för att en förutsättning för att upprätthålla suveräniteten är att myndigheter skyddar hela den kritiska försörjningskedjan och ser till att det finns s.k. exitstrategier när de använder sig av molntjänster.[105]

Innebörden av begreppet digital suveränitet har emellertid inte klargjorts. I tyska Digital Gipfels handlingsrekommendationer för hur Tyskland ska kunna upprätta digital suveränitet föreslås emellertid följande definition.[106]

En stats eller organisations digitala suveränitet inkluderar fullständig kontroll över lagrade och bearbetade data, liksom oberoende beslut om vem som får tillgång till data. Den inkluderar också förmågan att självständigt utveckla tekniska komponenter och system samt att förändra, kontrollera och genom andra funktioner komplettera dessa komponenter och system.[107]

Tyska förbundsministeriet för inrikesfrågor tillkännagav i september 2019 att ministeriet under de kommande åren kommer att arbeta för att stärka den offentliga förvaltningens digitala suveränitet. Detta ska ske bl.a. genom att beroendet av enskilda it-leverantörer minskas. Man överväger också alternativa program för att

---

[101] Detta tillkännagavs i en gemensam deklaration i samband med ett ministermöte 2016. Se Le ministère de l'Europe et des Affaires étrangères, *Déclaration du conseil franco-allemand de sécurité et de défense,* 2015.

[102] Europeiska rådet, En ny strategisk agenda för 2019-2024, juni 2019

[103] Europeiska unionens råd (Transport, Telecommunications and Energy Council), Conclusions on the Future of a highly digitised Europe beyond 2020: "Boosting digital and economic competitiveness across the Union and digital cohesion", 2019-06-07, s. 5, slutsats 7

[104] von der Leyen Ursula, Politiska riktlinjer för nästa europeiska kommission, 2019–2024, s. 5

[105] Robert Riemann vid EDPS, citerad vid the first European Software and Cloud Suppliers Customers Council, 2019-08-29. Se Huizing Lennart, *The Hague Forum for Cloud Contracting*, Privacy Company, 2019-10-24. En exitstrategi är en överenskommelse som beskriver de ekonomiska och tekniska förutsättningarna för att vid behov byta ut leverantören och flytta data.

[106] Digital Gipfel är ett samarbete mellan politik, näringsliv, vetenskap och samhälle, som administreras av närings- och energiministeriet (Bundesministerium für Wirtschaft und Energi). Samarbetet realiseras genom olika plattformar, varav ”Näringslivets innovativa digitalisering” (Innovative Digitalisierung der Wirtschaft) är en. Inom plattformen pågår projektarbete i fokusgrupper. Fokusgruppen ”Digital Suveränitet” redogjorde under 2018 för sina handlingsrekommendationer gällande digital suveränitet med särskilt fokus på artificiell intelligens. Se vidare Bundesministerium für Wirstschaft und energie, *Digital Gipfel*.

[107] Se Digital Gipfel, Digitale Souveränität und Künstliche Intelligenz – Voraussetzungen, Verantwortlichkeiten und Handlungsempfehlungen, 2018, s. 3

ersätta viss mjukvara från dessa leverantörer, efter avstämning på EU-nivå.[108] Förslagen konkretiserades i oktober 2019 i och med Project GAIA-X, som beskrivs som en federerad datainfrastruktur. Syftet uppges vara att säkra digital suveränitet, minska beroenden samt möjliggöra innovation och användning av molntjänster som inte strider mot europeisk rätt.[109]

För att möjliggöra privata tjänsteleverantörer har federala närings- och energidepartementet i Tyskland också publicerat kriterier som molntjänster ska uppfylla för att få kvalitetsstämpeln ”trusted cloud service”. Krav finns specificerade för leverantörens profil, möjligheterna till revision, hur avtal kan tecknas, underleverantörer, säkerhet, integritet, operativa processer, interoperabilitet, arkitektur och tjänsterna i sig.[110] De tjänster som uppfyller kriterierna publiceras offentligt efter att de certifierats.[111]

I Sverige beslutades nyligen en proposition, med förslag till ändringar i lagen om elektronisk kommunikation och offentlighets- och sekretesslagen för att kunna skydda Sveriges säkerhet vid användning av radiosändare. I propositionen för regeringen ett resonemang liknande det som förts av tyska Digital Gipfel. Begreppet digital suveränitet nämns förvisso inte uttryckligen. Regeringen menar dock att när skyddet för samhällsviktig infrastruktur utformas måste hänsyn tas till hur säkerhet och tillgänglighet kan påverkas av den åtkomst och kontroll över komponenter, system och infrastruktur som enskilt eller utländskt ägande eller utkontraktering medför. Det konstateras också att angrepp mot samhällsviktiga system från statliga eller statsstödda aktörer utgör allvarliga hot mot samhällets funktioner och hävdandet av vår suveränitet och territoriella integritet.[112]

---

[108] Bundesministerium des Innern, für Bau und Heimat, *BMI intensiviert Aktivitäten zur Stärkung der digitalen Souveränität in der öffentlichen Verwaltung*, 2019-09-19

[109] Federal Ministry for Economic Affairs and Energi (BMWi), *Project GAIA-X A Federated Data Infrastructure as the cradle of a vibrant European ecosystem*, s. 6–9, 12

[110] Federal Ministry for Economic Affairs and Energi (BMWi) *Criteria and catalogue for cloud services version 2*

[111] Federal Ministry for Economic Affairs and Energi (BMWi), *Trusted Cloud – Cloud providers*

[112] Prop. 2019/20:15, *Skydd av Sveriges säkerhet vid radioanvändning*, s. 26

Försäkringskassans slutsatser

- Det finns konflikter mellan tredjeländers myndigheters möjligheter att begära ut data som lagras hos tjänsteleverantörer under dess jurisdiktion och unionsrättsliga respektive svenska bestämmelser gällande dataskydd och sekretess.
- Utgångspunkten för diskussionen om samhällsbärande verksamhet i it-miljö bör dock inte vara dessa normkonflikter, utan de principiella frågor som uppstår när kontrollen över verksamhetens uppgifter överlämnas till privata företag eller andra länders myndigheter.
- Digitala verksamhetskritiska system i Försäkringskassans samhällsbärande verksamhet bör vara under den svenska statsförvaltningens kontroll.
- Försäkringskassan kommer inte att överlåta driften av digitala verksamhetskritiska system i samhällsbärande verksamhet till privata företag som står under jurisdiktion av ett land som har CLOUD Act-liknande lagstiftning. För it-system i viss verksamhet, t.ex. den säkerhetskänsliga, är Försäkringskassans mål för framtiden att vår it-drift ska ske i statlig regi.
- För att säkra samhällsbärande funktioner mot angrepp och minska beroendet av enskilda privata företag bör Sveriges digitala strategi kompletteras med ett ställningstagande om innebörden och värdet av digital suveränitet.
- I den mån publika molntjänster med privat drift används av svenska myndigheter ska myndigheterna bestämma villkoren för tjänsten. Sveriges offentliga aktörer bör genom samverkan nationellt och inom EU se till att de tjänster vi önskar använda erbjuds med villkor som följer svensk lagstiftning och säkerställer en adekvat säkerhetsnivå.

Publika molntjänster har stora fördelar

De publika molntjänster som marknaden erbjuder medför enligt vår mening många fördelar. Övergången till sådana molntjänster har i många fall lett till ökad verksamhetsnytta, ökad teknisk säkerhet och tillgänglighet till rimliga kostnader.[113] Det är därför önskvärt och ofta nödvändigt att myndigheterna kan använda tekniken som sådan och dra nytta av innovationsförmågan i den privata sektorn. De positiva effekterna får emellertid inte innebära att svenska myndigheter använder publika molntjänster utan att först bedöma konsekvenserna ur ett samhällsperspektiv och för individers personliga integritet. I följande avsnitt kommer vi bland annat att göra en sådan bedömning för Försäkringskassans del.

[113] Se Integritetskommittén, *Hur står det till med den personliga integriteten? – en kartläggning av Integritetskommittén* (SOU 2016:41), s. 110. Kommittén konstaterar dock att det även finns stora risker för myndigheter med molntjänster.

Normkonflikterna vid användning av molntjänster i privat regi är konstaterade

När det gäller CLOUD Act och annan liknande lagstiftning har debatten i Sverige till stor del handlat om förekomsten av konflikter mellan tredjelands myndigheters rätt att begära ut data som lagras hos tjänsteleverantörer under dess jurisdiktion å ena sidan och unionsrättsliga och svenska bestämmelser gällande dataskydd och sekretess å andra sidan. När det gäller dataskydd kan vi bara konstatera att Europeiska dataskyddsstyrelsen uttalat att det endast är i exceptionella fall ett utlämnande av personuppgifter enligt CLOUD Act-liknande lagstiftning är förenligt med GDPR. Med tanke på styrelsens sammansättning och uppdrag väger dessa uttalanden tungt i avvaktan på att EU-domstolen slutligt avgör frågan eller rättsläget ändras.[114]

Efter den analys som genomförts under arbetet med denna vitbok gör vi inte någon annan bedömning än den eSam och Kammarkollegiet gjort vad gäller förhållandet till offentlighets- och sekretesslagens röjandebegrepp. Att anlita tjänsteleverantörer som kan komma att lämna ut data till ett annat lands myndigheter kan inte heller anses vara förenligt med de grundläggande principerna i offentlighets- och sekretesslagen, som förutsätter att *den svenska myndigheten* (inte tjänsteleverantören eller en utländsk myndighet) ska göra en bedömning av utlämnandet *i varje enskilt fall*.[115]

Det faktum att samtliga sekretessreglerade uppgifter som tillgängliggörs för en tjänsteleverantör som omfattas av CLOUD Act eller liknande lagstiftning ska anses vara röjda, innebär att det inte går att lösa normkonflikten genom riskanalyser. En riskanalys skulle vad gäller sekretessreglerade uppgifter endast kunna mynna ut i en bedömning av vilka av dessa uppgifter myndigheten är beredd att röja för att kunna ta del av molntjänstens fördelar. Detta anser vi är en oacceptabel inställning. Samtliga sekretessreglerade uppgifter ska skyddas mot olagligt röjande och en prövning av en begäran om utlämnande måste som nämnts göras i varje enskilt fall, inte genom en övergripande riskanalys.

Kryptering kan i sig inte heller lösa normkonflikterna även om det erbjuder ett övergripande skydd mot antagonisters obehöriga tillgång. För det första går det inte att utesluta att en myndighet i ett annat land, som anser sig behörig att tillgå data, också anser sig ha rätt att tillgå krypteringsnycklar. Det är i nuläget inte möjligt att bedöma vilken utgång en sådan tvist skulle få. För det andra medför de krypteringsmetoder som skulle försvåra sådan tillgång att en stor del av tjänsternas funktionalitet samtidigt kraftigt försämras.

Normkonflikterna utgör bara en del av problembilden

En stor del av den svenska debatten har ägnats åt att försöka uppskatta i vilken omfattning svenska myndigheters data i publika molntjänster kan komma att lämnas ut till tredjeländer i enlighet med CLOUD Act eller liknande lagstiftning. Vi anser att diskussionen det senaste året om användning av privata företags publika molntjänster fått en olycklig slagsida mot den redan klargjorda frågan om vad

---

[114] Observera att ett avtal mellan EU och USA skulle kunna sätta Europeiska dataskyddsstyrelsens ställningstagande i ett annat ljus.

[115] Detta är en ordning som rimligen kommer att bestå. Förutsättningarna för den utredning som kommer att utreda säker och kostnadseffektiv it-drift för den offentliga förvaltningen är bl.a. att eventuella ändringar i offentlighets- och sekretesslagen inte får innebära någon ändring av, eller tillägg till, lagens bestämmelser om beslutsordning eller sekretessprövningens metodik. Se dir 2019:64.

dataskydds- och sekretessregleringen tillåter. Detta har lett till att andra mer trängande frågeställningar helt hamnat i skymundan.

Vi bedömer att det nu är hög tid att lyfta diskussionen till mer principiell nivå. Vi i den offentliga sektorn måste fråga oss, och besvara, hur vi ser på andra länders *möjligheter* att i enlighet med sin lagstiftning ensidigt skaffa sig åtkomst till data som tillhör svenska myndigheter. Hur dessa möjligheter nyttjas i nuläget är oväsentligt. Vi behöver också lyfta blicken från de normkonflikter som i nuläget föreligger och se andra länders möjligheter att få tillgång till svenska myndigheters data ur ett lämplighetsperspektiv. Det finns ett flertal frågeställningar som behöver tas fram och besvaras. Vi har hittills identifierat fyra:

Är det lämpligt att svenska myndigheter anförtror samhällsbärande verksamhet till en tjänsteleverantör som står under en annan stats jurisdiktion med möjligheter för den staten att utan svenskt medgivande ta del av uppgifter inom verksamheten?

Är det lämpligt att svenska myndigheter överlåter beslutet om att bestrida en begäran om utlämnande till andra länders myndigheter av sekretessreglerade uppgifter till en kommersiell part?

Är det lämpligt att svenska myndigheter inte har full kontroll och bestämmanderätt över vilka övriga länder som efter avtal med myndigheterna i tjänsteleverantörens ”hemland” kan komma att ta del av uppgifter inom vår samhällsbärande verksamhet?

Är det lämpligt att Sverige, till följd av den tillgång som uppkommer till information i molntjänster, i praktiken överlåter lagstiftningsmakt beträffande behandlingen av svenska myndigheters uppgifter till ett annat land?

Dessa frågor måste enligt vår mening beaktas i den allmänna lämplighetsbedömning som ska göras inför en myndighets val att använda sig av de publika molntjänster som marknadens aktörer erbjuder. Frågorna leder också över tankarna till en annan, mer angelägen, diskussion – den om vårt gemensamma ansvar för att säkra skyddet för verksamhet som är av betydelse för det svenska samhällets funktion.

Användning av publika molntjänster i privat regi ökar sårbarheten och integritetsriskerna

I denna vitbok ligger fokus på användning av publika molntjänster i privat regi. När det gäller det offentligas utkontraktering finns en mängd problem relaterade till skyddet av det svenska samhällets funktioner och den personliga integriteten, varav de följande är de vi identifierat som mest väsentliga.

Den allmänna sårbarheten ökar

Som vi tidigare redogjort för innebär användandet av publika molntjänster i privat regi, precis som andra typer av utkontraktering, att riskerna för antagonistiska it-angrepp från statliga eller statsstödda aktörer kan bli mer komplexa. Risken för att en stor mängd data från svenska myndigheter samlas hos en och samma tjänsteleverantör är också viktig att beakta, eftersom några få tjänsteleverantörer dominerar marknaden. Detta ökar sårbarheten, då störningar i en tjänst kan påverka många myndigheter samtidigt. När stora mängder information samlas på samma ställe ökar dessutom risken för angrepp i underrättelsesyfte.[116] De enskilda

[116] Riskerna med koncentration av data måste naturligtvis också beaktas när myndighetsinterna eller myndighetsövergripande tekniska lösningar utarbetas.

myndigheterna saknar information om enskilda tjänsteleverantörers samlade tillgång till svenska data. Om svensk offentlig sektor på detta sätt saknar helhetssyn finns ingen överblick över det samlade beroendet av olika tjänsteleverantörer, vilket ökar de totala riskerna för samhället ytterligare.

Dessa risker uppstår oavsett om tjänsterna erbjuds som molntjänster eller inte. Eftersom molntjänster i regel kan erbjudas till en större mängd kunder i samma fysiska infrastruktur är dessa risker emellertid större vid molntjänster än vid andra leveransmodeller.[117]

Risken för att obehöriga får åtkomst till data ökar

CLOUD Act och liknande lagstiftning har bidragit till att synliggöra debatten kring svenska myndigheters kontroll över egna data. Sådan lagstiftning är emellertid inte enda anledningen att iaktta försiktighet när det gäller användning av molntjänster i privat regi. Detta illustreras inte minst av avslöjandena 2013 av amerikanska myndigheters övervakning av bl.a. europeiska medborgare. Än viktigare att beakta är den underrättelseverksamhet som systematiskt bedrivs av bl.a. Ryssland, Kina och Iran och som kräver att svenska myndigheter bedriver ett systematiskt cybersäkerhetsarbete.[118] Mot bakgrund av nuvarande säkerhetsläge samt påtagligt förbättrade tekniska möjligheter måste risken för att utländska myndigheter tar del av uppgifter som hör till svensk samhällsbärande verksamhet, är sekretessreglerade eller skyddas av regleringen i GDPR tas på mycket större allvar än vad som hittills varit fallet.

Till detta kommer att tjänsteleverantörer tar del av telemetridata från kunder i den mjukvara de tillhandahåller, med hänvisning till att det behövs för att underhålla och förbättra tjänsten. Detta är viktigt att beakta inte minst vid publika molntjänster, där leverantören har större tillgång till data. Den analys som genomfördes på uppdrag av nederländska myndigheter indikerar att tjänsteleverantörerna hämtat in data i strid med GDPR, utan att det framgår av ingångna avtal och utan ett explicit medgivande från användaren.[119] Detta är djupt oroande och påverkar förtroendet för tjänsteleverantörernas förmåga att tillgodose de krav på skydd av uppgifter som bör ställas. Även om inhämtade telemetridata bara skulle användas av tjänsteleverantören i syfte att förbättra tjänstens funktionalitet, är det graverande att kunderna saknar insyn i processen, möjlighet att kontrollera vilken data som hämtats in och möjlighet att invända mot eller begränsa inhämtningen av sådan data. Det är vidare ytterst allvarligt att uppgifter om Sveriges samhällsbärande verksamhet och personuppgifter, även känsliga sådana, på detta sätt kan bli tillgängliga för obehöriga. När leverantörer hanterar personuppgifter på ett sätt som inte framgår av användarvillkoren och data tillgängliggörs för tredje part visar exemplet med

[117] Det bör noteras att riskerna med att data och funktioner koncentreras finns oavsett om tjänsteleverantören är offentlig eller privat.

[118] Se bl.a. Kristiansson Stefan, *Om underrättelsehotet mot Sverige, Frivärld*, Rapport nr 7 2019.

[119] Ministry of Justice and Security Strategic Vendor Management Microsoft, *DPIA Office 365 ProPlus version 190*5 *(June 2019) Data protection impact assessment on the processing of diagnostic data, se* vidare bilaga 8.

Cambridge Analytica att tillgång till stora mängder data kan få effekter på en demokratisk stats mest grundläggande intressen.[120]

Säkerhetsprövning av personal och uppföljningar omöjliggörs eller försvåras

När en svensk myndighet som bedriver säkerhetskänslig verksamhet använder sig av it-tjänster där teknisk personal inte befinner sig i Sverige, uppstår svårigheter relaterade till säkerhetsprövningen. Leverantörerna av globala publika molntjänster har i regel teknisk personal i en stor mängd länder för att kunna säkerställa hög tillgänglighet. Teknisk personal är sällan i förväg utsedda till att arbeta mot en specifik kund, samtidigt som säkerhetsprövningen ska göras på individbasis. Även om tjänsteleverantören skulle tillhandahålla namngiven personal för tjänsten, tillkommer att registerkontrollen, som är en viktig del av säkerhetsprövningen, inte är ett lika verksamt verktyg vad gäller personer som är bosatta i andra länder än Sverige. Detta måste då kompenseras genom en utökning av säkerhetsprövningens övriga delar. Det är också viktigt att reflektera över myndigheternas möjligheter att i praktiken följa upp ingångna säkerhetsskyddsavtal, när en publik, global molntjänst används och personal samt data finns i hela världen.

Riskbedömningar försvåras

Slutligen finns det när det gäller CLOUD Act ännu många oklarheter, bl.a. hur rättsakten kommer att tillämpas i förhållande till svenska myndigheters data och i vilken mån sådan data kommer att begäras ut. Därtill kommer osäkerheten kring vilka avvägningar mellan amerikanska och svenska intressen som amerikansk domstol kommer att göra efter en tjänsteleverantörs eventuella bestridande av en begäran om utlämnande. Det är dessutom oklart i vilken mån och med vilka länder amerikanska myndigheter kommer att ingå avtal med stöd av CLOUD Act om inhämtande av uppgifter.[121]

Mot denna bakgrund konstaterar Försäkringskassan att det i dagsläget inte går att överblicka konsekvenserna för en svensk myndighet som använder molntjänster där leverantören står under amerikansk jurisdiktion, vilket många av de kommersiella aktörerna gör. Det medför i sin tur att det blir svårt att inför en upphandling av molntjänster upprätta både konsekvensbedömningar enligt GDPR och risk- och sårbarhetsanalyser, som på ett rättvisande sätt åskådliggör de risker det innebär att överlåta delar av verksamheten till en privat tjänsteleverantör. CLOUD Act har fått tjäna som exempel, men problemen finns för samtliga molntjänster som erbjuds av en tjänsteleverantör i ett tredjeland vars lagstiftning ger det landets myndigheter tillgång till data som lagras hos tjänsteleverantörer under dess jurisdiktion. I och med att tjänster kan bestå av ett antal underliggande tjänster med olika leverantörer, som dessutom kan få förändrade ägarförhållanden, blir de framtida riskerna svåra att

---

[120] Cambridge Analytica var ett företag som erbjöd politiska konsulttjänster kombinerat med dataanalys och strategisk kommunikation. Företaget gick i konkurs efter att det framgått att de använt plattformen Facebook för att identifiera och påverka potentiella väljare i strid med användarvillkoren. Företagets verksamhet bedöms ha påverkat utkomsten i val i bl.a. USA, Storbritannien och Filippinerna. Läs mer: Auchard Eric, *Cambridge Analytica stage-managed Kenyan president's campaigns: UK TV, Reuters,* 2018-03-20, Cadwalladr, Carole, *The Great British Brexit robbery how our democracy was hijacked, The Guardian,* 2017-05-07 och Gutierrez Natashya, *Did Cambridge Analytica use Filipinos' Facebook data to help Duterte win?, Rappler,* 2018-04-05.

[121] Det kan dock noteras att ett första avtal, som slöts med Storbritannien i oktober 2019, ska läggas fram till USA:s kongress. Se Department of Justice, Office of Public Affairs, *U.S. And UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online,* 2019-10-03.

uppskatta. Detta inte minst när lagstiftningen i leverantörernas ”hemländer” förändras. Det är därutöver möjligt att en leverantörs ”hemland” ingår avtal med ett tredjeland som har CLOUD Act-liknande lagstiftning.

Integritetsrelaterade risker

Faktorer som ökar myndigheternas sårbarhet innebär samtidigt en ökad risk för den personliga integriteten. Som exempel kan nämnas riskerna för att obehöriga får tillgång till uppgifter, att det inte är möjligt att överblicka samtliga underleverantörer och att uppgifterna används för andra syften än de avtalade. Som Integritetskommittén konstaterat behandlar myndigheter ofta en stor mängd personuppgifter. Dessa tillhör ofta kategorin känsliga personuppgifter, eller är av annat integritetskänsligt slag. Detta innebär enligt vår mening att den förlust av kontroll över uppgifterna och den brist på insyn i hur uppgifterna behandlas som en molntjänst innebär, utgör en särskilt stor risk i integritetshänseende för just myndigheter.

Försäkringskassan ställningstagande för framtida användning av publika molntjänster i privat regi

Som framgår ovan finns det för närvarande många och allvarliga säkerhetsrelaterade problem kopplade till svenska myndigheters användning av många marknadsledande publika molntjänster i privat regi. Många molntjänster innebär visserligen en högre säkerhetsnivå ur ett tekniskt perspektiv och en högre tillgänglighet. Detta uppväger dock inte att dessa tjänster innebär att svenska myndigheter förlorar kontrollen över data. En självklar utgångspunkt för myndigheternas digitalisering bör enligt vår mening vara att vi inte ska acceptera en lägre skyddsnivå för den information som hanteras i molntjänster jämfört med den som hanteras i myndighetsinterna system. Till detta kommer lämplighetsfrågan.

När Försäkringskassan gör en sammantagen bedömning av de säkerhetsaspekter och de frågor kring lämplighet som identifierats i detta arbete finner vi – oavsett förekomsten av normkonflikter – att digitala verksamhetskritiska system i vår samhällsbärande verksamhet bör vara under den svenska statsförvaltningens kontroll. I praktiken innebär detta ställningstagande bland annat att Försäkringskassan inte kommer att överlåta driften av sådana system till privata företag som står under jurisdiktion av ett land som har CLOUD Act-liknande lagstiftning. Denna ståndpunkt kommer naturligtvis att behöva ses över om förslag från den nytillsatta statliga utredningen om säker och kostnadseffektiv statlig it-drift för den offentliga förvaltningen genomförs och sätter vårt ställningstagande i ett annat ljus.

Ställningstagandet innebär inte att ett statligt huvudmannaskap är enda lösningen. För vissa typer av samhällsbärande system skulle molntjänster i privat regi under rådande förutsättningar kunna upphandlas av privata företag i Sverige eller i vissa fall inom EU, förutsatt att upphandlingsrättsliga regler tillåter en sådan begränsning. Om så kan ske och om det är lämpligt att utnyttja tjänsteleverantörer utanför Sverige får avgöras i varje enskilt fall, utifrån verksamhetstyp och hur känsliga de uppgifter som hanteras i systemet är för bl.a. Sveriges säkerhet och enskilda. En förutsättning är naturligtvis också att avtalsvillkoren möjliggör en adekvat säkerhetsnivå och kontroll över att uppgifter inte förs över till tredjeland. I den mån privata tjänster används måste de självklart även uppfylla kraven i gällande lagstiftning.

Viss samhällsbärande verksamhet kräver enligt vår mening emellertid starkare statlig kontroll och styrning. För Försäkringskassans del kan nämnas den säkerhetskänsliga verksamheten. För it-system i sådan verksamhet kommer Försäkringskassans mål för framtiden att vara att vår it-drift ska ske i statlig regi.

För att en adekvat skyddsnivå för digital information ska bli verklighet i varje enskilt beslut hos varje enskild myndighet, krävs enligt Försäkringskassan också att Sverige som nation börjar föra en mer övergripande diskussion om de digitala skyddsvärdena.

Digital suveränitet – en väg mot minskad sårbarhet

Inledning

Allt större del av Sveriges samhällsbärande verksamheter är beroende av kontinuiteten i olika it-system. Det finns således all anledning att ta de risker som Säkerhetspolisen identifierat gällande teknikutvecklingen och utkontraktering av it på stort allvar. Skyddet av myndigheternas it-system är också en del av Sveriges försvarspolitiska inriktning, eftersom gränserna mellan civil och militär infrastruktur suddats ut i ett samhälle som blir alltmer teknikberoende.

Som framgår av Sveriges digitala strategi, måste svenska myndigheter ta ansvar för att digitala system är säkra och att den personliga integriteten värnas. Vi kan bara konstatera att detta inte går att genomföra utan en insikt om den sårbarhet vårt beroende av olika it-system medför och de beroenden som finns mellan olika typer av funktioner i samhället, oavsett om de kategoriserats som samhällsviktiga eller inte. Avgörande för att denna fråga ska få den uppmärksamhet den förtjänar är enligt vår bedömning att den del av suveräniteten som har att göra med kontroll över verksamhet i it-miljö synliggörs på ett mycket tydligare sätt än hittills.

Sveriges digitala suveränitet måste upp på agendan

Som MSB konstaterat tar begreppet nationell suveränitet sikte på statens förmåga att säkerställa kontrollen över territoriet, politiska beslutsprocesser och försörjning med förnödenheter. Om Sverige inte kan säkra suveräniteten, kan vi inte heller säkerställa samhällets funktioner eller skyddet för demokrati och rättssäkerhet.

I en alltmer digital värld får kontrollen över information i samhällsbärande verksamhet allt större betydelse för vårt lands möjlighet till oberoende. Mot den bakgrunden anser vi att det nu är hög tid att Sverige vidgar synen på vad suveränitet egentligen innebär. På samma sätt som Sverige behöver upprätthålla sin suveränitet i mer traditionell mening behöver vi nu klargöra hur den digitala suveräniteten ska upprätthållas.

Ett första steg på vägen har tagits av regeringen genom beslutet att ge Försvarets radioanstalt, Försvarsmakten, MSB och Säkerhetspolisen i uppdrag att göra förberedelser för att kunna skapa ett nationellt cybersäkerhetscenter.[122] Som Försvarsberedningen konstaterat ger en utvecklad förmåga på informations- och cybersäkerhetsområdet ökade möjligheter att upprätthålla suveräniteten.

För att upprätthålla den digitala suveräniteten krävs emellertid också att Sverige på en övergripande nivå identifierar vad vi anser bör ligga i begreppet. De diskussioner som förts inom EU och av dess medlemsstater – och som regeringen tangerat i propositionen om skydd av Sveriges säkerhet vid radioanvändning – har bl.a. handlat om självbestämmande och fullständig kontroll vad gäller hur myndigheternas it-system ska utformas och användas. De har också handlat om kontroll över data

[122] Försvarsdepartementet, *Uppdrag inför inrättandet av ett nationellt cybersäkerhetscenter*, Fö2019/01000/SUND, 2019-09-26

som lagras i dessa system och om vem som bereds tillgång till systemen. Detta anser vi kan tjäna som en utgångspunkt för att definiera hur vi i Sverige ska se på begreppet. Det handlar ytterst om att säkra våra samhällsbärande funktioner mot angrepp från andra stater och att minska beroendet av enskilda tjänster på marknaden. Syftet med detta är att skydda vårt samhälle och medborgarnas rättigheter.

Precis som när det gäller övriga delar av suveräniteten kommer det alltid att finnas olika typer av beroenden, både till andra stater och till privata aktörer. Det är inte säkert att digital suveränitet förutsätter ett fullständigt oberoende av privata och utländska parter. Utifrån den föränderliga omvärld vi upplever och den sårbarhet som beroendet av digitala system medför för oss som nation, måste vi emellertid ställa oss följande fråga.

Vilken kontroll är det rimligt att svenska myndigheter behåller över samhällsbärande funktioner i it-miljö?

När vi besvarar den frågan måste vi först och främst ta hänsyn till att risken för antagonistiska angrepp ökar ju mer kontroll vi lämnar ifrån oss. En annan viktig aspekt är att vi i varje enskilt beslut måste ta hänsyn till landets samlade beroende av en viss tjänsteleverantör eller en viss tjänst och de risker och inlåsningseffekter som ett sådant beroende medför. Vid bedömningen måste även flera faktorer som i dag är osäkra vägas in. Exempelvis kan vi i rådande säkerhetspolitiska läge inte utesluta risken för att Sverige dras in som tredje part i konflikter mellan andra länder och att detta påverkar vår digitala sårbarhet. Vi måste också beakta förtroendefrågan. Om svenska myndigheter sätter effektivitetsvinster och kortsiktiga ekonomiska vinster före skyddet för samhällets funktioner eller individers personliga integritet, riskerar vi i förlängningen allmänhetens förtroende för den offentliga förvaltningen.

För att säkra Sveriges digitala suveränitet krävs en tydlig styrning och en långsiktig handlingsplan

Oavsett vilken innebörd vi slutligen lägger i begreppet digital suveränitet är det avgörande att frågan förs på en myndighetsövergripande nivå och att det offentliga Sverige ses som en helhet. Idag utgörs Sveriges samlade strategi för att skydda våra samhällsbärande funktioner i it-miljö i praktiken av summan av enskilda myndigheters genomtänkta eller ogenomtänkta beslut. Försäkringskassan anser att det är en alldeles för passiv inställning till en fråga som är avgörande, både för hur statsförvaltningen ska kunna ta del av digitaliseringens möjligheter och för hur samhällsbärande digitala system ska kunna skyddas. Vi har nu möjlighet att ta efter Tysklands och Nederländernas goda initiativ att stärka den offentliga förvaltningens kontroll över information och minska beroendet av enskilda it-leverantörer. På så sätt kan vi vända den nuvarande utvecklingen, där kontrollen över samhällets funktioner riskerar att överlämnas till utländska företag och andra stater.

Vi är fast övertygade om att statsförvaltningen kan fortsätta dra nytta av alla digitaliseringens fördelar och samtidigt behålla sitt oberoende. Vi har stor tilltro till vad privata och offentliga innovatörer på relativt kort sikt kan åstadkomma, under förutsättning att det finns tillgängliga resurser och en tydlig inriktning för arbetet. Detta kan dock endast uppnås efter en noggrann analys baserad på fakta och beslut fattade på tillräckligt hög och central nivå.

Nu är således tid för aktiva beslut om hur Sveriges digitala suveränitet ska definieras och säkras. Det krävs tydlig statlig styrning och en långsiktigt hållbar handlingsplan för skyddet för de it-system som är en del av våra samhällsbärande funktioner. Det är därför vår bedömning att Sveriges digitala strategi bör kompletteras med ett

tydligare ställningstagande vad gäller den digitala suveräniteten. Först när sådan styrning finns på plats kan svenska myndigheter fullt ut ta det ansvar som krävs för att i praktiken säkra dessa verksamheter.

Tillgången till fysisk infrastruktur behöver skyndsamt utökas

För att i praktiken möjliggöra säkra it-tjänster för svenska myndigheter behöver de fysiska förutsättningarna säkerställas. Det saknas i dag ett uppdrag att säkerställa att den civila delen av statsförvaltningen har tillgång till säkra it-utrymmen, inkluderat säkra kommunikationer. Fortifikationsverket har analyserat förutsättningarna för att upprätta regionala datakluster. Därutöver har Post- och telestyrelsen på regeringens uppdrag lämnat förslag på en förvaltningsmodell för att möjliggöra samordning av säkra it-utrymmen. Inget av dessa förslag har emellertid ännu realiserats.

Det är givetvis ett steg i rätt riktning att regeringen nu tillsatt en utredning gällande säker och kostnadseffektiv it-drift för den offentliga förvaltningen.[123] Det är dock vår bedömning att sådana förslag kommer att kräva tillgång till fysisk infrastruktur som i dag inte finns och som kommer att ta flera år att realisera efter fattade beslut. Vi anser därför att det finns anledning för regeringen att parallellt med pågående utredning inleda realiseringen av de förslag som Fortifikationsverket och Post- och telestyrelsen lämnat. Om detta inte görs kommer genomförandet av en samordnad säker statlig it-drift att försenas, med risk för en ökad sårbarhet för myndigheternas it-drift. Vi vill i detta sammanhang också påpeka att en fysiskt säker infrastruktur, t.ex. i form av säkra it-utrymmen och kommunikationer, inte bör begränsas till statliga myndigheter. Det kan inte uteslutas att även kommunala myndigheter och vissa privata subjekt bedriver sådan samhällsbärande it-verksamhet som bör ha möjlighet till motsvarande skyddsnivå.

Sveriges offentliga aktörer måste tillsammans se till att molntjänster erbjuds med lagliga och lämpliga villkor

Vi är medvetna om att den hantering av publika molntjänster som vi efterfrågar skulle innebära att svenska myndigheter måste omvärdera redan gjorda investeringar och strategiska verksamhetsinriktningar. Detta påverkar även Försäkringskassan, som behöver se över genomförda, pågående och planerade projekt. Vi anser emellertid att Sveriges säkerhet och myndigheternas funktionssätt är av alltför stor betydelse för att underkastas avgörande hänsyn till redan gjorda investeringar. Vilka kostnader svenska samhället i slutänden skulle drabbas av om vi misslyckas med att upprätthålla skyddet för samhällsbärande verksamhet eller medborgarnas integritet, går dessutom inte att uppskatta på förhand. Med det beroende till tjänster med ogynnsamma eller t.o.m. olagliga villkor som svenska myndigheter för närvarande skaffat eller är på väg att skaffa, kommer det vidare att bli svårare att på sikt säkerställa att tjänsterna erbjuds med de villkor vi vill ha. Vi anser emellertid att det finns en lösning på problemet, men den måste hittas genom samverkan i offentlig sektor. Genom sådan samordning kan de privata leverantörerna också få en tydligare bild av den offentliga sektorns krav, vilket medför tydligare ekonomiska incitament att göra nödvändiga justeringar av tjänsterna.

[123] Se dir. 2019:64.

Svenska myndigheter kan agera gemensamt

Molntjänster innebär stora möjligheter att möta allmänhetens förväntningar på en effektiv och tillgänglig offentlig förvaltning. Rätt utformade kan de också vara starkt bidragande till att den offentliga sektorn når upp till regeringens högt ställda krav på att tillvarata digitaliseringens möjligheter.

Nyckelorden här är dock ”rätt utformade”. De tjänster svenska myndigheter använder måste vara anpassade till myndigheternas behov och säkerhetskrav, i stället för att utgå ifrån de redan existerande lösningar privata företag vill erbjuda oss. Kravet på en skyndsam digital utveckling får inte heller medföra att vi accepterar standardavtalsklausuler som inte uppfyller kraven i gällande lagstiftning eller i övrigt inte garanterar ett starkt skydd för säkerhet och integritet.

Hur åstadkommer vi då detta? Försäkringskassan vill här påminna om att den svenska offentliga sektorn sammantaget utgör en relativt stor beställare och därmed har goda möjligheter att ställa krav på de tjänster som ska upphandlas. Förutsättningen är dock att vi agerar gemensamt – en samlad statsförvaltning med ett tydligt budskap till marknaden är svår att bortse ifrån. Genom att vi gemensamt formulerar en kravställning kan vi inte bara påverka de existerande aktörerna på marknaden. Vi kan också skapa möjligheter för nya aktörer att erbjuda produkter som möter våra krav.

Vi står inte utan bra förebilder för detta arbete. Nederländernas regering har med framgång låtit förhandla fram ett tillägg till Microsofts standardavtal för Microsoft Office, i syfte att uppfylla GDPR:s krav. Nederländerna har som ambition att hela den offentliga sektorn inom EU ska kunna ansluta sig till tilläggsavtalet. Om svenska myndigheter står samlade i vår kravställning, bör vi således kunna dra nytta av Nederländernas framsteg. Det nederländska initiativet löser förvisso endast den del av lagkonflikterna som rör dataskyddet. Sverige bör därför också, både nationellt och på myndighetsnivå, ansluta sig till de initiativ till samarbete som nu växer fram mellan EU-ländernas myndigheter i syfte att förhandla fram bättre avtalsvillkor med de stora tjänsteleverantörerna.[124] På så sätt ökar våra möjligheter att få marknaden att erbjuda tjänster där kontrollen behålls inom myndigheten i stället för att överlåtas till privata aktörer eller tredjeländer.[125] På samma sätt bör vi kunna agera för att se till att privata tjänster anpassas till övrig svensk lagstiftning och till den säkerhetsnivå som det offentliga Sverige behöver kräva för att behålla kontrollen över sin verksamhet. I Nederländerna har det nämnda tilläggsavtalet förhandlats fram av en utpekad myndighet med ett samlat ansvar att företräda Nederländernas intressen. I det arbete Sverige har att göra har vi allt att vinna på att samordna oss på liknande sätt.

[124] Som exempel kan nämnas The Hague forum for Cloud contracting, som anordnas av Nederländernas justitiedepartement och Strategic Vendor Management, nästa gång under våren 2020.

[125] En sådan tjänst skulle kunna utgöras av en privat molntjänst på plats hos kund, vilket i korthet innebär att myndigheten köper in en tjänst som används på myndighetens egna servrar.

Sammanfattning

Sammanfattningsvis anser Försäkringskassan att den svenska debatten om myndigheters förutsättningar att använda publika molntjänster som tillhandahålls av privata aktörer inte haft rätt fokus. Försäkringskassan anser förvisso att det finns normkonflikter mellan andra länders lagstiftning om tillgång till uppgifter som finns hos tjänsteleverantörer och svensk rätt respektive EU-rätt. Men tyngdpunkten i diskussionen bör varken ligga här eller på om dessa länders myndigheter använder sina möjligheter att få tillgång till uppgifter som tillhör svenska myndigheter. Istället bör lämplighetsaspekter och myndigheternas gemensamma ansvar för att skydda samhällsbärande verksamhet vara utgångspunkter för debatten.

Vi bedömer att publika molntjänster i privat regi som används i samhällsbärande verksamhet ökar verksamhetens allmänna sårbarhet och riskerna för att obehöriga får åtkomst till data. Därutöver orsakar användningen av sådana molntjänster stora – ibland oöverkomliga – svårigheter i säkerhetsprövningen av de personer som ska befatta sig med säkerhetskänslig verksamhet och uppföljningar av ingångna säkerhetsskyddsavtal. Dessutom medför CLOUD Act och liknande lagstiftning svårigheter när det gäller att upprätta rättvisande konsekvensbedömningar eller risk- och sårbarhetsanalyser. Till detta kommer det principiella problemet med att svenska myndigheter avhänder sig kontrollen över verksamhetens uppgifter till privata företag eller andra länders myndigheter.

Mot den bakgrunden kommer Försäkringskassan under rådande förutsättningar inte att överlåta driften av sådana system till privata företag som står under jurisdiktion av ett land som har CLOUD Act-liknande lagstiftning. I vilken mån upphandling av tjänster kan ske av svenska eller europeiska aktörer får avgöras utifrån en lämplighetsbedömning i varje fall, där bl.a. verksamhetstyp, uppgifternas känslighet och möjliga avtalsvillkor beaktas. För t.ex. den säkerhetskänsliga verksamheten kommer Försäkringskassans mål för framtiden emellertid att vara att vår it-drift ska ske i statlig regi.

För att svenska myndigheter ska kunna upprätthålla en adekvat skyddsnivå för digital information krävs enligt Försäkringskassan vidare att Sverige som nation börjar diskutera innebörden och värdet av digital suveränitet. En utgångspunkt i dessa diskussioner bör enligt vår mening vara att våra samhällsbärande funktioner ska säkras mot angrepp och att beroendet av enskilda tjänster på marknaden ska minskas. På detta sätt kan vi förvalta det förtroende vi fått av medborgarna att ta hand om samhällets funktioner och individers känsliga personuppgifter. Vi anser således att det nu är dags att Sverige som nation går från en passiv hållning till en aktiv strategi för digital suveränitet och en målbild för vad detta innebär i myndigheternas dagliga verksamhet. För detta krävs en tydlig styrning och en långsiktig handlingsplan som omfattar hela den offentliga sektorn. En sådan handlingsplan bör även inkludera säker infrastruktur, t.ex. i form av säkra it-utrymmen och säkra kommunikationer, och en långsiktigt hållbar förvaltningsmodell för denna infrastruktur.

Ett sådant synsätt behöver inte betyda att digitaliseringen av offentlig sektor avstannar. Vi är övertygade om att privata och offentliga innovatörer med rätt resurser och förutsättningar kan bidra till att svenska myndigheter kan fortsätta dra fördel av digitaliseringens alla möjligheter utan att äventyra säkerheten för samhällsbärande verksamhet. Genom samverkan både nationellt och inom EU kan svenska myndigheter vidare se till att de privata tjänster vi väljer att använda anpassas till våra önskemål, lagstiftningen och en säkerhetsnivå som gör att vi kan behålla kontrollen över vår verksamhet. Utgångspunkten måste alltid vara att myndigheterna, och inte privata företag, bestämmer villkoren för de tjänster som upphandlas.

Referenser

Abelson Harold m.fl., *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications*, (MIT-CSAIL-TR-2015-026), November 2015

Access Now, European Digital Rights (EDRi), Electronic Frontier Foundation, Panoptykon Foundation, *Letter to US Congress*, 2018-03-19 https://edri.org/files/cross-borderaccesstodata/lettertocongress_CLOUDAct_20180319.pdf

Amnesty International USA, Electronic Frontier Foundation och Human Rights Watch m.fl., Brev till amerikanska kongressen, 2018-03-12. https://www.eff.org/document/coalition-letter-opposing-cloud-act (Hämtad 2019-09-02)

Auchard Eric Reuters, *Cambridge Analytica stage-managed Kenyan president's campaigns: UK TV*, 2018-03-20 https://www.reuters.com/article/us-facebook-cambridge-analytica-kenya/cambridge-analytica-stage-managed-kenyan-presidents-campaigns-uk-tv-idUSKBN1GV300 (Hämtad 2019-11-10)

Autoriteit Persoonsgegevens (Dutch DPA), *Summary of Investigation Report Public Version Microsoft Windows 10 Home and Pro*, Augusti 2017

AWS, *AWS Government cloud för amerikanska staten* https://aws.amazon.com/govcloud-us/ (Hämtad 2019-09-10)

AWS, *Global Infrastructures Regions and AZs* https://aws.amazon.com/about-aws/global-infrastructure/regions_az/?p=ngi&loc=2 (Hämtad 2019-09-10)

AWS, *Information Request Report* https://d1.awsstatic.com/certifications/Information_Request_Report_June_2019.pdf (Hämtad 2019-09-10)

AWS *Protection Data using encryption* https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html (Hämtad 2019-11-10)

Bellanger Pierre, *De la souveraineté en général et de la souveraineté numérique en particulier*, Les Échos, 2011-08-30.

Blix Fredrik och Brolin Richard, *Grönt ljus för kommuner, regioner och statliga myndigheter att överväga molntjänster*, Cybercom Group, 2019-07-04 https://www.cybercom.com/sv/Om-Cybercom/Bloggar/digital-sakerhet/gront-ljus-for-kommuner-regioner-och-statliga-myndigheter-att-overvaga-molntjanster/ (Hämtad 2019-09-04)

Bondcap, *Internet Trends 2019* https://www.bondcap.com/report/itr19 (Hämtad 2019-09-20)

Bundesministerium des Innern, für Bau und Heimat, *BMI intensiviert Aktivitäten zur Stärkung der digitalen Souveränität in der öffentlichen Verwaltung*, 2019-09-19 https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2019/09/digitale-souveraenitaet-oeff-verwltg.html (Hämtad 2019-09-20)

Bundesministerium für Wirstschaft und energie, *Digital Gipfel* https://www.de.digital/DIGITAL/Navigation/DE/Service/Digital-Gipfel/Digital-Gipfel.html (Hämtad 2019-09-20)

Butler Brandon, *What is hybrid cloud computing? The benefits of mixing private and public cloud services, Networkworld*, 2017-10-17 https://www.networkworld.com/article/3233132/what-is-hybrid-cloud-computing.html (Hämtad 2019-11-09)

Cadwalladr Carole, *The Great British Brexit robbery how our democracy was hijacked, The Guardian*, 2017-05-07 *https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy* (Hämtad 2019-11-10)

Corey Varma, *Encryption vs. Fifth Amendment* http://www.coreyvarma.com/2015/07/encryption-vs-fifth-amendment/ (hämtad 2019-09-17)

Council of Bars and Law Societies of Europe, *CCBE Assessment of the U.S. CLOUD Act*, 2019-02-28

Daskal Jennifer, Unpacking the CLOUD Act, *EUCRIM, 2019-01-31* https://eucrim.eu/articles/unpacking-cloud-act/ (Hämtad 2019-09-02)

Department of Justice, Office of Public Affairs, *U.S. And UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online*, 2019-10-03 https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists (Hämtad 2019-10-09)

Digital Gipfel, Plattform Innovative Digitalisierung der Wirtschaft: Fokusgruppe Digitale Souveränität in einer vernetzten Gesellschaft, *Digitale Souveränität und Künstliche Intelligenz – Voraussetzungen, Verantwortlichkeiten und Handlungsempfehlungen*, 2018 https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2018/p2-digitale-souveraenitaet-und-kuenstliche-intelligenz.pdf?__blob=publicationFile&v=5 (Hämtad 2019-10-15)

Director of National Intelligence, *Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 2013-06- 08 https://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf (Hämtad 2019-09-03)

Ds 2017:66, *Motståndskraft – Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025*

Ds 2018:6, *Granskning av Transportstyrelsens upphandling av it-drift*

E-delegationen, *Strategi för myndigheternas arbete med e-förvaltning* (SOU 2009:86)

E-delegationen, *Så enkelt som möjligt för så många som möjligt* (SOU 2011:67)

EDPB-EDPS, *Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection*, 2019-07-10

Ekonomistyrningsverket, *It-kostnadsmodell* (2014:50), 2014-10-01

Electronic Frontier Foundation, *EFF and 23 Groups Tell Congress to Oppose the CLOUD Act*, 2018-03-11
https://www.eff.org/deeplinks/2018/03/eff-and-x-groups-tell-congress-oppose-cloud-act (Hämtad 2019-08-08).

Electronic frontier Foundation, EFF in the United States Court of Appeals for the Eleventh Circuit Case: 11-12268

Electronic frontier Foundation, *The U.S. CLOUD Act and the EU: A Privacy Protection Race to the Bottom*, 2018-04-09
https://www.eff.org/de/deeplinks/2018/04/us-cloud-act-and-eu-privacy-protection-race-bottom#_ftn1 (Hämtad 2019-08-07)

eSamverkansprogrammet, *Kompletterande information om molntjänster*, 2019-09-20

eSamverkansprogrammet, *Rättsligt uttalande om röjande och molntjänster*, VER 2018:57, 2018-10-23

eSamverkansprogrammet, *Röjandebegreppet enligt offentlighets- och sekretesslagen*, VER 2015-190, 2015-12-17

Europaparlamentet, Europaparlamentets resolution av den 5 juli 2018 om huruvida ett adekvat skydd säkerställs genom skölden för skydd av privatlivet i EU och USA (2018/2645(RSP))

Europaparlamentet, *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices* (PE 583.137)

Europeiska dataskyddsstyrelsen, *Riktlinjer 2/2018 för undantagen i artikel 49 enligt förordning 2016/679*, antagna den 25 maj 2018

Europeiska kommissionen, *Brief of the European Commission on behalf of the European Union as amicus curiae in support of neither Party in the case United States v. Microsoft Corp*

Europeiska rådet, *En ny strategisk agenda för 2019-2024*, juni 2019
https://www.consilium.europa.eu/media/39936/a-new-strategic-agenda-2019-2024-sv.pdf (Hämtad 2019-10-01)

Europeiska unionens råd (Transport, Telecommunications and Energy Council), *Conclusions on the Future of a highly digitised Europe beyond 2020: "Boosting digital and economic competitiveness across the Union and digital cohesion"*, 2019-06-07,
https://www.consilium.europa.eu/media/39667/st10102-en19.pdf

Federal Ministry for Economic Affairs and Energi (BMWi), *Criteria and catalogue for cloud services version 2*

Federal Ministry for Economic Affairs and Energi (BMWi), *Project GAIA-X A Federated Data Infrastructure as the cradle of a vibrant European ecosystem*

Federal Ministry for Economic Affairs and Energi (BMWi), *Trusted Cloud – Cloud providers*
https://www.trusted-cloud.de/en/cloud-services (Hämtad 2019-11-10)

Fedramp, *Third Party Assessment Organization (3PAO)*
https://www.fedramp.gov/assessors/ (Hämtad 2019-09-20)

Finansdepartementet, *Regleringsbrev för Ekonomistyrningsverket 2014*

Finansdepartementet, *Uppdrag att erbjuda samordnad säker statlig it-drift* (FI2017/03257/DF)

Finansdepartementet, *Uppdrag att föreslå en förvaltningsmodell för skyddade it-utrymmen* (Fi2017/03084/DF)

Försvarets radioanstalt, *Årsrapport 2018*

Försvarsdepartementet, *Uppdrag inför inrättandet av ett nationellt cybersäkerhetscenter* (Fö2019/01000/SUND), 2019-09-26

Försvarsmakten, *Godkända kryptoapparater september 2019*
https://www.forsvarsmakten.se/sv/organisation/hogkvarteret/militara-underrattelse-och-sakerhetstjansten/kryptografiska-funktioner/ (Hämtad 2019-10-01)

Försvarsutskottets betänkande 2014/15:FöU11

Försäkringskassan, *Delredovisning samordnad och säker statlig it-drift,* (046278-2017), 2017-11-24

Försäkringskassan, *Delredovisning samordnad och säker statlig it-drift,* (046278-2017), 2018-10-29

Gartner, Market Insight: *Finding Cloud Opportunities in the government,* 2017-06-27 ID: G00327356

Gellman Barton and Soltani Ashkan, *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say, The Washington Post, 2013-10-30*
https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html (Hämtad 2019-09-24)

Google, *Begäran om användarinformation*
https://transparencyreport.google.com/user-data/overview (Hämtad 2019-09-05)

Gutierrez, Natashya, *Did Cambridge Analytica use Filipinos' Facebook data to help Duterte win?, Rappler,* 2018-04-05
https://www.rappler.com/nation/199599-facebook-data-scandal-cambridge-analytica-help-duterte-win-philippine-elections (Hämtad 2019-11-10)

Hellberg, Islam, Karlsson, *Säkerhet vid molnlösningar,* Örebro Universitet och Myndigheten för samhällsskydd och beredskap

Hern Alex, *Facebook agrees to pay fine over Cambridge Analytica scandal, The Guardian,* 2019-10-30
https://www.theguardian.com/technology/2019/oct/30/facebook-agrees-to-pay-fine-over-cambridge-analytica-scandal (Hämtad 2019-11-10)

Huizing Lennart, *The Hague Forum for Cloud Contracting,* Privacy Company, 2019-10-24
https://www.privacycompany.eu/en/the-hague-forum-for-cloud-contracting/ (Hämtad 2019-10-2)

Infrastrukturdepartementet, *Säker och kostnadseffektiv it-drift för den offentliga förvaltningen* (Dir. 2019:64)

Infrastrukturdepartementet, *Ändring av uppdrag att erbjuda samordnad och säker statlig it-drift* (I2019/02515/DF)

Integritetskommittén, *Hur står det till med den personliga integriteten? – en kartläggning av Integritetskommittén* (SOU 2016:41)

International Organization for Standardization, ISO/IEC 2382:2015(en) Information technology — Vocabulary

Justitiedepartementet, Lagrådsremiss *Hemlig dataavlyssning,* 2019-10-24

Justitiedepartementet, *Uppdrag till Myndigheten för samhällsskydd och beredskap att genomföra riktade utbildningsinsatser på informationssäkerhetsområdet till offentlig sektor* (Ju2019/03057/SSK)

Justitiedepartementet, *Uppdrag till Myndigheten för samhällsskydd och beredskap att ta fram en struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen* (Ju2019/03058/SSK, Ju2019/02421/SSK)

Kammarkollegiet, *Förstudierapport Webbaserat kontorsstöd,* DNR 23.2-6283-18, 2019-02-22

Kristiansson Stefan, Om underrättelsehotet mot Sverige, *Frivärld*, Rapport nr 7 2019.

Le ministère de l'Europe et des Affaires étrangères, *Déclaration du conseil franco-allemand de sécurité et de défense, 2015*
https://www.diplomatie.gouv.fr/IMG/pdf/_16-04-07_declaration_cfads__cle8eaec8.pdf

Markander Mikael, Strömavbrott hos molnjätten – kunder förlorade data, *ComputerSweden,* 2019-09-06
https://computersweden.idg.se/2.2683/1.723105/kunder-drabbade-stromavbrott-aws (Hämtad 2019-09-10)

Maurer Tim m.fl *Technological Sovereignty: Missing the Point? An Analysis of European Proposals after June 5, 2013,* New America's Open Technology Institute och the Global Public Policy Institute (GPPi) https://www.gppi.net/media/Maurer-et-al_2014_Tech-Sovereignty-Europe.pdf

Microsoft, Sveriges Kommuner och Landsting m.fl., Öppet seminarium på Almedalen 2019, *CLOUD Act – hinder eller ej* https://www.youtube.com/watch?v=tqCRZt81bZk (Hämtad 2019-09-04)

Microsoft, *Configure ADRMS restrictions* https://docs.microsoft.com/sv-se/azure/information-protection/configure-adrms-restrictions (Hämtad 2019-09-23)

Microsoft, *Konfigurera diagnostikdata för Windows i din organisation*, 2019 https://docs.microsoft.com/sv-se/windows/privacy/configure-windows-diagnostic-data-in-your-organization (Hämtad 2019-09-24)

Microsoft, *Law Enforcement Requests Report* https://www.microsoft.com/en-us/corporate-responsibility/lerr (Hämtad 2019-09-10)

Microsoft *Molntjänster och säkerhet*, 2018-12-13 https://news.microsoft.com/sv-se/2018/12/13/molntjanster-och-sakerhet/ (Hämtad 2019-09-04)

Microsoft, *Office 365 Government cloud för amerikanska staten* https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/office-365-us-government/office-365-us-government (Hämtad 2019-09-23)

Microsoft, *Service encryption with Customer Key for Office 365 FAQ*, 2018-07-31 https://docs.microsoft.com/en-us/office365/securitycompliance/service-encryption-with-customer-key-faq (Hämtad 2019-09-24)

Microsoft, *Ta med din egen nyckel (BYOK) information om Azure Information Protection, 2019-09-22* https://docs.microsoft.com/sv-se/azure/information-protection/byok-price-restrictions (Hämtad 2019-09-25)

Ministerie van Justitie en Veiligheid, *Verificatie op de uitvoering van het overeengekomen verbeterplan met Microsoft* (Ons kenmerk 2635551), 2019-07-01

Ministry of Justice and Security Strategic Vendor Management Microsoft, DPIA Office 365 ProPlus version 1905 (June 2019) Data protection impact assessment on the processing of diagnostic data

Myndigheten för samhällsskydd och beredskap, *Handlingsplan för skydd av samhällsviktig verksamhet*, MSB597, dec 2013

Myndigheten för samhällsskydd och beredskap, *Upphandling till samhällsviktig verksamhet – en vägledning*, MSB1275, september 2018.

Myndigheter för samhällsskydd och beredskap, *Vägledning för identifiering av samhällsviktig verksamhet*, MSB1408, juni 2019

Myndigheten för samhällsskydd och beredskap, *Vägledning för risk- och sårbarhetsanalyser*, MSB245, april 2011

Myndigheten för samhällsskydd och beredskap, *Övergripande inriktning för samhällsskydd och beredskap*, MSB708, juni 2014

Näringsdepartementet, *Med medborgaren i centrum – Regeringens strategi för en digitalt samverkande statsförvaltning* (N2012:37)

Office of the Director of National Intelligence United States Intelligence Activities (Federal Register Vol. 40, No. 235 (December 8, 1981), amended by EO 13284 (2003), EO 13355 (2004), and EO 13470 (2008))

Pensionsmyndigheten, *Molntjänster i staten – en ny generation av outsourcing* (med bilagan Juridisk analys av myndigheters informationshantering i molnet), 2016

Post- och telestyrelsen, *Förslag till en förvaltningsmodell för skyddade it-utrymmen* (Dnr: 17-8280)

Proposition 2014/15:109, *Försvarspolitisk inriktning – Sveriges försvar 2016-2020*

Proposition 2019/20:15, *Skydd av Sveriges säkerhet vid radioanvändning*

Punke Michael, AWS and the CLOUD Act, *AWS Security Blog*, 2019-05-27 https://aws.amazon.com/blogs/security/aws-and-the-cloud-act/ (Hämtad 2019-09-02)

Regeringen, *Säker och kostnadseffektiv it-drift för den offentliga förvaltningen*, dir 2019:64

Regeringens skrivelse 2010/11:138, *R*iksrevisionens granskning av it inom statsförvaltningen och statliga it-projekt

Riksdagens protokoll 2014/15:117

Riksrevisionen, *Granskning om IT-förvaltning delvis missförstådd*, 2017-09-26 https://www.riksrevisionen.se/om-riksrevisionen/kommunikation-och-media/nyhetsarkiv/2017-09-26-granskning-om-it-forvaltning-delvis-missforstadd.html (Hämtad 2019-09-30)

Riksrevisionen, *IT inom statsförvaltningen – har myndigheterna på ett rimligt sätt prövat frågan om outsourcing bidrar till ökad effektivitet?* (RiR 2011:4)

Statens servicecenter, *En gemensam statlig molntjänst för myndigheternas it-drift – Delrapport i regeringsuppdrag om samordning och omlokalisering av myndighetsfunktioner*, 2017-02-07 (DNR 10052-2016/1121)

Strategic Vendor Management Microsoft for the Dutch Government and Ministerie van Veiligheid en Justitie, *EU Software and Cloud Supplier Customer Council* https://www.youtube.com/watch?v=96EVKaosVps&feature=youtu.be (Hämtad 2019-09-25)

Sveriges kommuner och Landsting, *Molntjänster och konfidentialitetsbedömning*, https://skl.se/download/18.3414859716e267c4fe2ad9d8/1572961426896/Molntja%CC%88nster%20och%20konfidentialitetsbedo%CC%88mning_191105.pdf (Hämtad 2019-11-09)

Sveriges Kommuner och Landsting, *Ställningstagande om informationshantering i vissa molntjänster*, ärendenummer 19/00087, 2019-04-12

Säkerhetspolisen, *Informationssäkerhet* https://www.sakerhetspolisen.se/sakerhetsskydd/informationssakerhet.html (Hämtad 2019-09-05).

Säkerhetspolisen, *Personalsäkerhet*
https://www.sakerhetspolisen.se/sakerhetsskydd/personalsakerhet.html (Hämtad 2019-09-05)

Säkerhetspolisen, *Säkerhetsskydd vid upphandlingar och affärsavtal*,
https://www.sakerhetspolisen.se/sakerhetsskydd/sakerhetsskydd-vid-upphandlingar-och-affarsavtal.html (Hämtad 2019-09-06)

Säkerhetspolisen, *Vägledning i säkerhetsskydd – Introduktion till säkerhetsskydd*
https://www.sakerhetspolisen.se/download/18.7acd465e16b4e0e54c64d/1560777315837/Vagledning-Introduktion-till-sakerhetsskydd.pdf (Hämtad 2019-09-05)

Säkerhetspolisen, *Vägledning i säkerhetsskydd – personalsäkerhet*, juni 2019

Säkerhetspolisen, *Årsbok 2017*

Säkerhetspolisen, *Årsbok 2018*

The App Association m.fl., *Öppet brev till Attorney General Barr*, 2019-06-21
https://www.bsa.org/files/policy-filings/06212019bsaletteruseulea.pdf (Hämtad 2019-09-02)

Totalförsvarets forskningsinstitut och Fortifikationsverket, *Strategisk utblick 8 – Totalförsvarets tillväxt –utmaningar och möjligheter, Så kan vi skydda Sveriges säkerhetskänsliga it-tjänster*, (FOI 4773), maj 2019

Transportstyrelsen, *Kartläggning av hanteringen av vissa uppgifter* (TSG 2017-2515), 2018-01-23

United States Department of commerce, *Security and Privacy Controls for Federal Information Systems and Organizations*
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf (Hämtad 2019-10-15)

United States Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, White Paper, april 2019

United States District Court for the District of Vermont., No. 2:06-mj-91, 2009 WL 424718 Feb. 19, 2009. MEMORANDUM of DECISION In re Grand Jury Subpoena to Sebastien Boucher

Utredningen om hemlig dataavläsning, *Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet*, (SOU 2017:89)

Utredningen om it-brottskonventionen, *Europarådets konvention om it-relaterad brottslighet* (SOU 2013:39)

von der Leyen Ursula, *Politiska riktlinjer för nästa europeiska kommission, 2019-2024*

Bilaga 1 Utkontraktering av svensk statlig it-drift – en historisk belysning

Redan i E-delegationens första betänkande 2009 lyftes förslaget att regeringen ska ställa krav på myndigheterna att ta fram en strategi för sin försörjning av it-tjänster, en s.k. sourcingstrategi. Strategin skulle väga in myndigheters specifika situation. De parametrar som skulle styrka valet av sourcing var främst kostnad, kvalitet och flexibilitiet.[126]

År 2011 genomförde Riksrevisionen en analys av om statliga myndigheter i tillräcklig utsträckning övervägde utkontraktering för att säkra behoven av it.[127] Riksrevisionens slutsats var att utkontraktering inte prövas i tillräcklig omfattning. Som orsak angavs att myndigheter inte kan redovisa sina it-kostnader, att det finns brister i intern styrning, att det saknas effektivitetskrav på myndigheternas it-avdelningar, att beställarkompetensen är låg, att det råder oklarheter kring informationsklassning av ”känslig information”, att kunskapsspridning mellan myndigheter brister och att regeringen inte underlättat utkontraktering. Riksrevisionen rekommenderade därför regeringen att ta fram riktlinjer och ökat erfarenhetsutbyte mellan myndigheter.[128]

Regeringen uppgav i sitt svar på rapporten att frågan gällande myndigheters utkontraktering av it-tjänster skulle beredas vidare. Regeringen menade också att det var önskvärt att en större del av myndigheternas it-behov tillfredsställs med hjälp av utkontraktering.[129]

Riksrevisionen kom senare att i samband med diskussionerna efter Transportstyrelsens utkontraktering av it-drift att kommentera att tolkningen av deras granskning delvis missförståtts.[130]

I regeringens digitialiseringsstrategi 2012 lyftes att E-delegationen under 2012-2013 skulle genomföra en fördjupad förstudie.[131] E-delegationen beskrev att syftet med förstudien var att identifiera och beskriva möjligheterna till effektivisering av myndigheternas it-drift över departements- och myndighetsgränser, inklusive förslag på hur sådana lösningar kan utformas. Förstudien skulle belysa hur staten i framtiden bör driva, utbyta eller köpa och sälja it-tjänster inom den statliga sektorn, inklusive värdering av olika sourcingmodeller. Den skulle också belysa kraven på

---

[126] E-delegationen, *Strategi för myndigheternas arbete med e-förvaltning*, (SOU 2009:86), s. 15ff

[127] I detta dokument används termen utkontraktering. I många fall används ordet outsourcing, vilket är den engelska termen. Offshoring är ett begrepp som används för utkontraktering där it-leveransen genomförs i ett annat land.

[128] Riksrevisionen, *IT inom statsförvaltningen – har myndigheterna på ett rimligt sätt prövat frågan om outsourcing bidrar till ökad effektivitet?* (RiR 2011:4), s. 63ff

[129] Regeringens skrivelse 2010/11:138, *Riksrevisionens granskning av it inom statsförvaltningen och statliga it-projekt*

[130] Riksrevisionen, *Granskning om IT-förvaltning delvis missförstådd*, 2017-09-26

[131] Näringsdepartementet, *Med medborgarens centrum – Regeringens strategi för en digitalt samverkande statsförvaltning* (N2012:37), s. 22

informationssäkerhet samt omfatta en hinderanalys och förslag på införandestrategi.[132] Förstudierapporten publicerades emellertid aldrig.

År 2014 gav regeringen Ekonomistyrningsverket i uppdrag att utveckla myndigheternas arbete kring it-kostnader, it-investeringar och outsourcing och regeringen meddelade i årsredovisningen att ärendet avseende sourcingstrategi därmed var att betrakta som slutberett på Regeringskansliet.[133] Uppdraget till Ekonomistyrningsverket var att ta fram en it-kostnadsmodell. Myndigheten skulle också överväga hur modellen kan innehålla uppföljning av strategiska val, såsom strategi för it-försörjning.[134] Ekonomistyrningsverkets rapport 2014 beskrev statens kostnader för it.[135]

Parallellt med Ekonomistyrningsverkets uppdrag fick Pensionsmyndigheten våren 2015 i uppdrag av regeringen att analysera och värdera potentialen för användning av molntjänster i staten samt att redovisa vilka risker och hinder som eventuellt finns förknippade med användning av molntjänster i statlig verksamhet. Analysen skulle också visa hur användning av molntjänster kan bidra till målet om en enklare, öppnare och effektivare förvaltning. Pensionsmyndigheten poängterade i rapporten att molntjänster har vissa begränsningar för statens verksamhet och att ju känsligare informationen var och ju fler integrationer som finns, desto svårare blir outsourcing. Varje myndighet rekommenderades genomföra en laglighetskontroll och att säkerställa att en god informationssäkerhet kan upprätthållas.[136] De juridiska aspekterna belystes i en särskild bilaga. I den lyfte Pensionsmyndigheten frågan om nationell säkerhet och poängterade att den behövde ett större fokus. Pensionsmyndigheten rekommenderade därför även en fortsatt utredning av statliga molntjänster.[137]

Statens servicecenter fick 2016 i uppdrag av regeringen att analysera möjligheterna till just statliga molntjänster. Rapporten överlämnades i februari 2017. Statens servicecenters slutsats var att merparten av de statliga myndigheternas it-drift bör samordnas i en statlig molntjänst, som skulle erbjuda myndigheterna två tjänster: datorkraft och lagring.[138]

Regeringen gav 2017 Post- och telestyrelsen i uppdrag att ta fram förslag på en förvaltningsmodell för skyddade it-utrymmen.[139] Post- och telestyrelsen slutrapporterade i februari 2018 och föreslog en fördjupad analys följt av en implementation av en förvaltningsmodell som skulle möjliggöra en samordning av säkra it-utrymmen.[140]

---

[132] E-delegationen, *Så enkelt för så många som möjligt* (SOU 2011:67), s. 30

[133] Finansdepartementet, *Årsredovisning för staten 2012*, s. 115, Finansdepartementet, *Årsredovisning för staten 2013*, s. 116 och Finansdepartementet, *Årsredovisning för staten 2014*, s. 124.

[134] Finansdepartementet, *Regleringsbrev för Ekonomistyrningsverket 2014*, s. 5

[135] Ekonomistyrningsverket, *It-kostnadsmodell* (2014:50)

[136] Pensionsmyndigheten, *Molntjänster i staten – en ny generation av outsourcing, 2016*, s. 73ff

[137] Pensionsmyndigheten, *Molntjänster i staten – en ny generation av outsourcing, 2016*, Bilagan *Juridisk analys molntjänster i staten*, s. 58ff

[138] Statens servicecenter, *En gemensam statlig molntjänst, Delrapport i regeringsuppdrag om samordning och omlokalisering av myndighetsfunktioner* (DNR 10052-2016/1121)

[139] Finansdepartementet, *Uppdrag att föreslå en förvaltningsmodell för skyddade it-utrymmen*, (DNR Fi2017/03084/DF)

[140] Post- och telestyrelsen, *Förslag till en förvaltningsmodell för skyddade it-utrymmen* (Dnr: 17-8280)

Post- och telestyrelsens uppdrag kompletterades i augusti 2017 med ett uppdrag till Försäkringskassan att erbjuda samordnad säker statlig it-drift till lämpliga funktioner och myndigheter mellan 2017 och 2020.[141] Försäkringskassan skulle även ta fram förslag på lämpliga former för samordnad statlig it-drift efter 2020. Försäkringskassan betonade i sina delrapporter 2017 och 2018 att behovet av stöd avseende it-drift är stort hos statliga myndigheter och att framför allt mindre myndigheter har behov av ett totalåtagande.[142] Försäkringskassan pekade i sin återrapportering 2018 på vikten av att realisera den förvaltningsmodell för säkra it-utrymmen som Post- och telestyrelsen föreslog 2018.[143]

Fortifikationsverket genomförde 2016-2019 ett antal förstudier avseende tillgången på it-utrymmen med fortifikation. En förstudie finansierad av MSB analyserade ett bredare behov från statsförvaltningen för att kunna möjliggöra samordnade it-tjänster. Efter den genomförda förstudien konstaterade Fortifikationsverket att en väsentlig del av uppbyggnaden av den svenska totalförsvarsförmågan handlar om skydd av samhällsviktig verksamhet och inte minst för samhällsviktiga it-system.[144]

I september 2019 presenterade regeringen åtgärder för stärkt informations- och cybersäkerhet. Bland annat fattades beslut om inrättande av ett nationellt cybersäkerhetscenter med syfte att stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera cyberhot. Myndigheten för samhällsskydd och beredskap fick i uppdrag att genomföra riktade utbildningsinsatser på området och att ta fram en struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen.[145]

Dessa uppdrag kompletterades med regeringens initiativ att tillsätta en utredning gällande säker och kostnadseffektiv it-drift för den offentliga förvaltningen. Syftet med utredningen är enligt direktiven 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. I direktiven pekar regeringen på osäkerhet i fråga om de rättsliga förutsättningarna för utkontraktering, främst gällande tolkningen av när en uppgift ska anses vara röjd enligt sekretesslagstiftningen. Regeringen bekräftar att denna oro har förstärkts i och med CLOUD Act. Regeringen konstaterar att om ett uppgiftsutlämnande inkluderar personuppgifter, behöver den utkontrakterande myndigheten också säkerställa att den behandling av personuppgifter som ska utföras är förenlig med dataskyddsregleringen. Regeringen identifierade även att en särskild utmaning för

---

[141] Finansdepartementet, *Uppdrag att erbjuda samordnad och säker statlig it-drift* (Fi2017/03257/DF)

[142] Med totalåtagande avses tillgång till en extern it-avdelning som hanterar utveckling, förvaltning och drift så som en intern it-avdelning skulle göra. Se Försäkringskassan, *Delredovisning samordnad och säker statlig it-drift*, (046278-2017), 2017-11-24 och Försäkringskassan, *Delredovisning samordnad och säker statlig it-drift*, (046278-2017), 2018-10-29

[143] Post- och telestyrelsen, *Förslag till en förvaltningsmodell för skyddade it-utrymmen*, Dnr: 17-8280

[144] Totalförsvarets forskningsinstitut och Fortifikationsverket, S*trategisk utblick 8 – Totalförsvarets tillväxt – utmaningar och möjligheter, Så kan vi skydda Sveriges säkerhetskänsliga it-tjänster*, (FOI 4773), maj 2019

[145] Justitiedepartementet, *Uppdrag till Myndigheten för samhällsskydd och beredskap att genomföra riktade utbildningsinsatser på informationssäkerhetsområdet till offentlig sektor*, (Ju2019/03057/SSK), Justitiedepartementet, *Uppdrag till Myndigheten för samhällsskydd och beredskap att ta fram en struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen* (Ju2019/03058/SSK, Ju2019/02421/SSK) och Försvarsdepartementet, *Uppdrag inför inrättandet av ett nationellt cybersäkerhetscenter*, (Fö2019/01000/SUND)

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, d.v.s. ett land utanför EU- och EES-området.[146]

I samband med fastställandet av kommittédirektiven beslutade regeringen även att förlänga Försäkringskassans uppdrag att erbjuda samordnad säker statlig it-drift. Regeringen framförde att på så sätt svarar löptiden för Försäkringskassans uppdrag bättre mot utredningstiden för den nytillsatta utredningen och tiden som behövs för efterföljande hantering av utredningens förslag.[147]

[146] Infrastrukturdepartementet, *Säker och kostnadseffektiv it-drift för den offentliga förvaltningen* (Dir. 2019:64)

[147] Infrastrukturdepartementet, *Ändring av uppdrag att erbjuda samordnad och säker statlig it-drift* (I2019/02515/DF)

Bilaga 2 Begreppet molntjänst och uppskattad användning av publika molntjänster i svensk offentlig sektor

Molntjänster kan definieras på flera olika sätt. I den här rapporten används definitionen från ISO/IEC 17788:2014 (ISO, 2014) där molntjänst definieras som

”en eller flera funktioner som ingår i molnbaserade datortjänster […] och anropas via ett definierat gränssnitt” där en molnbaserad datortjänst är ”ett koncept som möjliggör nätverksåtkomst till en skalbar och elastisk pool av delade fysiska eller virtuella resurser som via självbetjäning levereras och administreras på begäran. Resurserna i denna definition inkluderar bland annat servrar, operativsystem, nätverk, mjukvara, applikationer och lagringsutrustning”.[148]

De huvudegenskaper (kännetecken) som ISO och SIS har definierat och som ytterligare ramar in begreppet listas nedan:

- Användarna kan komma åt fysiska och virtuella resurser från olika platser med hjälp av olika klienter och enheter så länge det finns tillgängliga nätverk.
- Kunderna betalar endast för de resurser de nyttjar.
- Fysiska eller virtuella resurser fördelas på ett sådant sätt att flera användare delar miljö, men deras beräkningar och data är isolerade från och oåtkomliga för varandra.
- Tjänsterna ger användarna möjlighet att göra vad de behöver göra, när de behöver göra det, utan att kräva ytterligare mänskliga användarinteraktioner eller administrationskostnader. Molntjänster kan i vissa fall beställas, sättas upp och börja användas helt utan mänsklig interaktion.
- Fysiska eller virtuella resurser kan levereras snabbt och elastiskt, i vissa fall automatiskt, så att resurserna snabbt kan ökas eller minskas och där den upplevda kundnyttan är att inte behöva oroa sig för begränsade resurser eller för kapacitetsplanering.
- Molntjänstleverantörer kan stödja fleranvändande samtidigt som de kan använda abstraktion som ett sätt att dölja komplexiteten i processen för kunden.

Molntjänster kan erbjudas olika kundgrupper. I det fall molntjänsten bara kan tillgängliggöras en kund (som kan vara den egna organisationen) benämns molntjänsten som en privat molntjänst (private cloud). I detta sammanhang används inte ordet privat som en beskrivning av tjänsteleverantörens rättsliga status. En molntjänst som erbjuds en avgränsad grupp kunder kallas partnermolntjänst (partner cloud/community cloud), medan en molntjänst som erbjuds en bredare grupp eller

[148]ISO/IEC 17788:2014 är den internationella standard som dels tillhandahåller en översikt över vad molntjänster innebär, dels innehåller en rekommendation av termer och definitioner att använda i detta sammanhang. Se Hellberg, m.fl *Säkerhet vid molnlösningar*.

allmänheten kallas publik molntjänst (public cloud). Det är dock viktigt att betona att ”publik” i detta sammanhang inte innebär att allmänheten har tillgång till all data i tjänsten utan varje kund ska endast ha tillgång till ”sin” data. I svensk statsförvaltning finns exempel på alla tre typer av molntjänster. Försäkringskassan använder till exempel privata molntjänster för att erbjuda vissa funktioner till de egna medarbetarna. Inom ramen för det statliga regeringsuppdraget Samordnad säker statlig it-drift erbjuds de myndigheter med vilka Försäkringskassan inlett samverkan vissa tjänster genom partnermolntjänster. Många myndigheter använder också publika molntjänster som Office 365 för att tillhandahålla kontorsstöd. I sammanhanget kan även nämnas begreppet Hybrid Cloud som betecknar när flera modeller används kompletterande för att leverera tjänster mot en kund.[149]

Det finns tre internationellt etablerade typer av molntjänster som beskriver tre olika funktionsområden. Då definitionen är globalt spridd används de engelska termerna och förkortningarna.

Infrastructure as a Service (IaaS) innebär it-infrastrukturella tjänster i nätet. Kunden kan skapa och använda resurser hos en eller flera molntjänstleverantörer i form av fysisk hårdvara såsom servrar, nätverk, lagringsutrymme, arkitekturell uppbyggnad, lastbalansering, beräkning etc. Kunden tillhandahåller själv de plattformar och applikationer som körs i infrastrukturen. Kunden har inte kontroll över den underliggande infrastrukturen men äger alltså kontroll över t.ex. operativsystem, lagring och utvecklade och utrullade applikationer i infrastrukturen.

Platform as a Service (PaaS) innebär att leverantören tillhandahåller applikations-plattformar via internet eller annat nät, för användare att installera sina egna applikationer i. Ett exempel på en PaaS-tjänst är utvecklingsmiljöer som tjänst.

Software as a Service (SaaS) innebär att leverantören tillhandahåller mjukvara som tjänst, dvs. färdiga eller konfigurerbara applikationer över internet eller annat nät. Tjänstetypen kallas ibland även Applications as a service (AaaS) Denna tjänstetyp kan levereras på flera sätt och vara tillgänglig genom t.ex. en webbläsare. Leverantören står för allt underhåll.[150]

Enligt den undersökning Pensionsmyndigheten gjorde 2016 var SaaS-lösningar den i särklass vanligaste modellen[151] och det finns inget som tyder på att det är en något som förändrats.

Eftersom nyttor upplevs både hos kunden och hos leverantören har molntjänster blivit en allt vanligare leveransmodell. På ett globalt plan används molntjänster nu för att hantera uppskattningsvis 22 % av all organisationell data. Utvecklingen har gått mycket snabbt och inom några år kan molntjänster globalt användas för större datamängder än data som lagras lokalt eller på egna servrar.[152]

Tre amerikanska företag har en mycket stark position på marknaden för molntjänster. Amazon Web Services (AWS), Microsoft och Google erbjuder publika molntjänster. Företagen har ett brett utbud av publika molntjänster som erbjuds både privatpersoner och större organisationer. Tillväxttakten är hög och den samlade

---

[149] Butler, *What is hybrid cloud computing? The benefits of mixing private and public cloud services*

[150] Pensionsmyndigheten, *Molntjänster i staten*, s. 13ff

[151] Pensionsmyndigheten, *Molntjänster i staten*, s. 56ff

[152] Bondcap, *Internet Trends 2019*, s. 153

vinsten för dessa tre tjänster var första kvartalet 2019 strax under 47 miljarder dollar.[153]

Ett antal större leverantörer, inklusive AWS och Microsoft har upprättat särskilda privata molntjänster för amerikanska myndigheter.[154] Detta för att möta de krav som amerikanska myndigheter ställer på sina leverantörer.[155] Motsvarande strategier återfinns i flera länder med motivationen att suveräniteten ska säkras.[156]

Sveriges myndigheter har också en ökande användning av molntjänster. I en studie finansierad av Myndigheten för samhällsskydd och beredskap 2018 uppgav 75 % av de tillfrågade kommunerna och myndigheterna att de använde minst en upphandlad molntjänst. Bland kommunala myndigheter använde över 80 % minst en publik molntjänst.[157]

Den främsta uppgivna orsaken till valet av molntjänster var hög flexibilitet men även kostnadsfördelar uppgavs som viktiga för mer än hälften av respondenterna.[158]

För kommuner uppgavs utbildningsadministration vara den vanligaste tjänsten, medan statliga myndigheter uppgavs ha en större spridning i typen av tjänst.

Respondenterna gavs också möjlighet att uppge orsaken till varför de hindrades från att använda molntjänster. De främsta skälen var bristen på kontroll och lagstiftning. Över 20 % uppgav att de var på väg att börja använda dessa tjänster.[159]

Många av de publika molntjänsterna bygger på att kunder och användare finns globalt och ska ha tillgång under hela dygnet och alla dagar på året. För att möta dessa krav finns anläggningar och personal i regel på spridda platser över hela världen. Den exakta placeringen av olika anläggningar och personal är i regel företagshemligheter, men viss information finns tillgänglig publikt. Till exempel uppger AWS att de finns lokaliserade i USA, Brasilien, Sverige, Frankrike, Tyskland, Danmark, Finland, Storbritannien, Norge, Italien, Tjeckien, Österrike, Polen och Schweiz, Sydafrika, Förenade Arabemiraten, Israel, Indien, Hongkong, Kina, Malaysia, Filipinerna, Japan, Korea, Singapore och Taiwan samt i Australien.[160]

Vilket lands lag som är tillämplig blir en utmaning när informationsägare, data som lagras respektive teknisk personal som kan få tillgång till data finns i flera olika länder. Detta åskådliggörs bland annat genom den debatt som förs kring brottsbekämpande myndigheters möjligheter att få tillgång till data i publika molntjänster.

---

[153] Bondcap, *Internet Trends 2019*, s. 116

[154] Microsoft, *Microsoft Office 365 Government cloud för amerikanska staten* och AWS, *AWS Government cloud för amerikanska staten*. Samtliga amerikanska myndigheter använder inte dessa molntjänster och flera amerikanska myndigheter använder de publika molntjänsterna som dessa företag erbjuder.

[155] Fedramp, *Third Party Assessment Organization (3PAO) och United States Department of commerce, Security and Privacy Controls for Federal Information Systems and Organizations*

[156] Gartner, *Market Insight: Finding Cloud Opportunities in Government*, ID: G00327356, 2017-06-27

[157] Hellberg m.fl, *Säkerhet vid molnlösningar*, s. 25

[158] Hellberg, m.fl, *Säkerhet vid molnlösningar*, s. 28

[159] Hellberg m.fl, *Säkerhet vid molnlösningar*, s. 33

[160] AWS, *Global Infrastructures Regions and AZs*

Bilaga 3 Konflikter mellan tredjeländers lagstiftning, EU-rätt och nationell rätt

En stor del av den svenska debatten kring CLOUD Act och liknande lagstiftning har handlat om de normkonflikter som uppstår mellan sådan lagstiftning å ena sidan och EU-rätt och svensk rätt å andra sidan. I denna bilaga redogör vi för de diskussioner som förts på områdena offentlighet- och sekretess samt dataskydd.

Offentlighet och sekretess

Offentlighets- och sekretesslagen – en översikt

Den grundlagsstadgade rätten att ta del av allmänna handlingar begränsas genom offentlighets- och sekretesslagen (2009:400).[161] Om sekretess råder för en uppgift är det förbjudet att röja den, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt.[162] Röjandeförbudet gäller för myndigheter, men också för en person som fått kännedom om uppgifter genom att hen för det allmännas räkning deltar i en myndighets verksamhet, t.ex. på grund av anställning eller uppdrag hos myndigheten.[163] Sekretess gäller som huvudregel inte bara i förhållande till enskilda utan också mellan myndigheter samt i förhållande till utländska myndigheter och mellanfolkliga organisationer.[164]

Av särskilt intresse i förhållande till CLOUD Act och annan liknande lagstiftning är möjligheten att lämna ut sekretessbelagda uppgifter till utländska myndigheter. Ett sådant utlämnande får bara ske i enlighet med föreskrift i lag eller förordning eller om uppgiften i motsvarande fall skulle fått lämnas ut till en svensk myndighet. I det sistnämnda fallet krävs också att den utlämnande myndigheten gör en prövning av om det är förenligt med svenska intressen att uppgiften lämnas till den utländska myndigheten.[165]

Det finns dock särskilda sekretessbrytande bestämmelser. Dessa kan möjliggöra ett utlämnande av uppgifter som annars är sekretessbelagda, om det behövs för att myndigheten ska kunna utföra sina uppgifter eller för att tillgodose enskildas berättigade behov.[166]

Innan en svensk myndighet gör sekretessreglerade uppgifter tillgängliga för en tjänsteleverantör, måste myndigheten bl.a. analysera om detta innebär ett röjande av uppgifter i den mening som avses i offentlighets- och sekretesslagen. Myndigheterna måste vidare ständigt säkerställa att sekretessreglerna upprätthålls. Det måste således

---

[161] 2 kap. 1-2 §§ TF

[162] *3 kap. 1 § OSL*

[163] 2 kap. 1 § OSL

[164] 8 kap. 1-3 §§ OSL

[165] 8 kap. 3 § OSL

[166] Sekretessbrytande bestämmelser som bryter all sekretess eller sekretess enligt väldigt många sekretessbestämmelser finns i 10 kap. OSL. I övrigt finns sekretessbrytande bestämmelser i anslutning till den eller de berörda sekretessbestämmelserna i avdelning IV och V OSL.

finnas beredskap för att nya regelverk, t.ex. i andra länder, kan komma att påverka de it-lösningar som svenska myndigheter valt att använda.[167]

Konflikten mellan lagstiftning liknande CLOUD Act och offentlighets- och sekretesslagen

År 2015 uttalade eSamverkansprogrammets rättsliga expertgrupp (nedan eSam) att uppgifter normalt inte ska anses röjda i offentlighets- och sekretesslagens mening, trots att de gjorts tekniskt tillgängliga för en tjänsteleverantör om

- tjänsteleverantören enligt avtal inte får ta del av eller vidarebefordra uppgifterna och
- omständigheterna i övrigt medför att det är osannolikt att detta ändå sker.[168]

Med anledning av CLOUD Act och annan liknande lagstiftning gjorde eSam 2018 ett nytt rättsligt uttalande. Detta uttalande tog specifikt sikte på röjandebegreppet vid användande av molntjänster som lyder under utländsk lagstiftning. eSam menade att sekretessreglerade uppgifter får anses vara röjda om de görs tekniskt tillgängliga för en tjänsteleverantör som till följd av t.ex. ägarförhållanden är bunden av regler i ett annat land, enligt vilka tjänsteleverantören kan bli skyldig att överlämna information utan att internationell rättshjälp anlitats eller annan laglig grund föreligger enligt svensk rätt. eSam gjorde bedömningen att det i sådana situationer inte kan anses vara osannolikt att uppgifterna kan komma att lämnas till utomstående. Samma bedömning gjordes för de situationer där ägarförhållanden eller geografisk placering av en tjänsteleverantörs tekniska hjälpmedel ger anledning att befara att mänskliga rättigheter (till exempel skyddet för privatlivet) eller det allmännas intressen (t.ex. rikets säkerhet) inte skulle säkerställas om svenska myndigheters data hade tillgängliggjorts för tjänsteleverantören.[169]

eSam kommenterade i september 2019 sitt rättsliga uttalande och anförde, något förenklat, bl.a. följande. I ett första steg måste den rättsliga regleringen av parternas mellanhavande ha utformats på ett hållbart sätt. Det ska finnas en juridiskt bindande och sanktionerad avtalssekretess och leverantören får inte vara bunden av regler i främmande rätt om att lämna ut uppgifter utan en föregående sekretessprövning eller annan laglig grund enligt svensk rätt för ett utlämnande. Finns det brister i denna del innebär ett tillgängliggörande för leverantören att uppgifterna anses vara röjda i offentlighets- och sekretesslagens mening. Någon sannolikhetsbedömning blir då inte aktuell. Finner en myndighet däremot att en planerad utkontraktering skulle få en stabil juridisk grund ska det göras en bedömning av om det är osannolikt att tjänsteleverantören eller dennes personal, som inte får ta del av eller vidarebefordra uppgifterna, i praktiken ändå kommer att befatta sig med uppgifterna på ett otillåtet sätt.

---

[167] Se vidare Kammarkollegiet, *Förstudierapport Webbaserat kontorsstöd,* Dnr 23.2-6283-18, 2019-02-22, s. 35.

[168] eSamverkansprogrammet, *Röjandebegreppet enligt offentlighets- och sekretesslagen, VER 2015-190,* 2015-12-17

[169] eSamverkansprogrammet, *Rättsligt uttalande om röjande och molntjänster*, VER 2018:57, 2018-10-23

Kammarkollegiet instämde 2019 i eSams bedömning.[170] Kammarkollegiet uttalade vidare att det inte är förenligt med offentlighets- och sekretesslagen att en tjänsteleverantör som anlitats av en svensk myndighet lämnar ut sekretessbelagda uppgifter till en utländsk myndighet i enlighet med CLOUD Act eller liknande lagstiftning. Detta beror – något förenklat – på att det inte finns någon särskild föreskrift i lag eller förordning som medger ett sådant utlämnande. Det är heller inte möjligt att säkerställa att en uppgift i motsvarande fall skulle fått lämnas ut till en svensk myndighet eller att säkerställa att svenska intressen tillgodoses.[171] Kammarkollegiet konstaterade också att en svensk myndighet som låter företag som lyder under ett regelverk liknande CLOUD Act hantera sekretessreglerade uppgifter, synes ge det utländska regelverket företräde framför svensk lagstiftning.[172]

En annan uppfattning har bl.a. Microsoft. Bolaget menar att CLOUD Act medför ännu tydligare argument för att det ska anses vara osannolikt att en tjänsteleverantör som anlitats av svenska myndigheter tar del av eller vidarebefordrar sekretessreglerade uppgifter. Microsoft menar således att ett ”automatiskt röjande” inte sker i dessa situationer och framhåller att man inte bara ska se till det utländska ägandet utan göra en mer nyanserad bedömning utifrån bl.a. avtalsåtaganden, historik och teknisk arkitektur. Microsoft hänvisar också till att antalet ärenden där bolaget fått en begäran om att lämna ut uppgifter som lagras utanför USA:s gränser är mycket få.[173] Denna omständighet uppmärksammas även av Cybercom Group, som är underleverantör till AWS. Cybercom menar att verkligheten nu ser annorlunda ut än när eSam gjorde sitt rättsliga uttalande 2018. Cybercom pekar på att vissa av molntjänsterna erbjuds från svenska it-hallar och att det finns säkerhetsarrangemang, t.ex. kryptering, som myndigheten helt kontrollerar själv gentemot molntjänstleverantören. Bolaget menar också att det krävs detaljerad kunskap om den it-säkerhetstekniska lösning som molntjänstleverantörerna erbjuder för att kunna avgöra frågan om det är osannolikt att information obehörigen röjs. Cybercoms slutsats är att det nu inte finns några hinder mot att kommuner, regioner och statliga myndigheter överväger användning av molntjänster, även om de är utlandsägda.[174] Bolaget menar att samma uppfattning framkommit vid ett slutet rundabordsamtal på Almedalen 2019, där representanter från centrala svenska myndigheter inom dataskydd och cybersäkerhet, generaldirektörer för statliga myndigheter samt representanter för Sveriges Kommuner och Landsting (SKL) deltog.[175]

SKL har, bl.a. med anledning av eSams ställningstagande 2018, uttalat att marknadsdrivna molntjänster – även sådana med ägarförhållande utomlands – är en nödvändig del av digitaliseringen. SKL påtalar också att en stor andel av Sveriges kommuner och regioner redan använder sådana molntjänster, som i vissa fall har

---

[170] Kammarkollegiet, *Förstudierapport Webbaserat kontorsstöd*, Dnr 23.2-6283-18, 2019-02-22, s. 35. Observera att Kammarkollegiets ställningstagande endast gällde eSams uttalanden 2015 och 2018.

[171] Jfr 8 kap. 3 § OSL

[172] Kammarkollegiet, *Förstudierapport Webbaserat kontorsstöd*, s. 32–33

[173] Se bl.a. Microsoft, *Molntjänster och säkerhet*, 2018-12-13, Sveriges Kommuner och Landsting m.fl., Öppet seminarium på Almedalen 2019, *CLOUD Act – hinder eller ej.*

[174] Cybercom hänvisar här även till rapporter från två separata advokatbyråer som analyserat det rättsliga läget och ska ha kommit till slutsatsen att den nuvarande regleringen ger utrymme för att överväga användning av utlandsägda molntjänster, men att en analys måste ske i varje enskilt fall. Bolaget menar också att personer bakom eSams uttalande 2018 nu ska ha gett uttryck för en något mildare tolkning av uttalandet.

[175] Blix Fredrik och Brolin Richard, *Grönt ljus för kommuner, regioner och statliga myndigheter att överväga molntjänster*, Cybercom Group, 2019-07-04

upphandlats av statliga myndigheter. Osäkerheten gällande de rättsliga frågorna uppges redan ha medfört en inbromsning av digitaliseringen och gjort att avsevärda resurser läggs på tolkning och anpassning istället för nyttorealisering. Eftersom det handlar om mycket stora – kommande och redan gjorda – investeringar menar SKL att det finns behov av en nationell, sammanhållen inriktning i frågan för offentliga organisationer. SKL anser vidare att avsaknad av nationell samsyn kring rättsläget för molntjänster med utländskt ägande kan leda till stora problem för digital samverkan mellan offentliga aktörer och i förlängningen till minskade möjligheter att leverera de tjänster som allmänheten förväntar sig. I den mån det finns sådana begränsningar för informationshantering, lagring eller kommunikation av viss känslig eller sekretessreglerad information som beskrivs i uttalande av eSam, menar SKL att detta måste klargöras genom kompletterad eller ändrad lagstiftning.[176]

EU:s dataskyddsförordning

När data som innehåller personuppgifter förs över till ett tredjeland (ett land utanför EU) efter en begäran i enlighet med CLOUD Act eller annan liknande lagstiftning utgör detta en personuppgiftsbehandling. Under vilka förutsättningar en sådan behandling får ske regleras 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 (allmän dataskyddsförordning), nedan kallad GDPR.

Personuppgiftsansvarig och personuppgiftsbiträde

Den som är personuppgiftsansvarig ansvarar för att behandlingen av personuppgifter sker i enlighet med GDPR. Personuppgiftsansvarig är den som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Den personuppgiftsansvarige kan anlita ett personuppgiftsbiträde, som behandlar personuppgifterna för den personuppgiftsansvariges räkning. Ett sådant biträde finns alltid utanför den personuppgiftsansvariges organisation och får bara behandla personuppgifter enligt instruktion från den personuppgiftsansvarige. Den personuppgiftsansvarige får i sin tur endast anlita personuppgiftsbiträden som ger tillräckliga garantier för att behandlingen genomförs i enlighet med GDPR och för att den registrerades rättigheter skyddas.[177]

När en myndighet köper molntjänster av en tjänsteleverantör är myndigheten personuppgiftsansvarig. Genom ett personuppgiftsbiträdesavtal ges tjänsteleverantören instruktioner om syftet med behandlingen och hur denna ska ske. Leverantören är personuppgiftsbiträde så länge den behandlar personuppgifterna för myndighetens räkning och i enlighet med avtalet. Skulle tjänsteleverantören behandla personuppgifterna för något annat syfte än de som fastställts genom avtalet bör leverantören betraktas som personuppgiftsansvarig.[178] Innan en svensk myndighet anlitar en tjänsteleverantör som personuppgiftsbiträde, måste myndigheten dock analysera om detta innebär en risk för att personuppgifter behandlas i strid med GDPR.

---

[176] Sveriges Kommuner och Landsting, *Ställningstagande om informationshantering i vissa molntjänster*, ärendenr 19/00087, 2019-04-12

[177] Artiklarna 4.7, 4.8, 5.2, 26.1, 28.1 och 28.3 i GDPR

[178] Se artikel 28.10 i GDPR samt Kammarkollegiet, *Förstudierapport Webbaserat kontorsstöd,* s. 14.

Förhållandet mellan CLOUD Act och EU:s dataskyddsförordning

Såväl Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen som EU-kommissionen har uttalat sig i frågan om det är förenligt med GDPR att en tjänsteleverantör lämnar ut personuppgifter som lagras inom EU till en utländsk myndighet, t.ex. i brottsbekämpande syfte. Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen förespråkar ett tvåstegstest för att försäkra sig om att en överföring av personuppgifter till ett tredjeland uppfyller GDPR:s krav. För det första måste det finnas en rättslig grund för personuppgiftsbehandlingen och samtliga övriga krav i förordningen måste vara uppfyllda, t.ex. vad gäller de allmänna principerna om proportionalitet, riktighet, lagringsminimering och säkerhet.[179] För det andra måste överföringen vara i överensstämmelse med bestämmelserna i kapitel V i GDPR, som uttömmande reglerar under vilka förutsättningar personuppgifter får föras över till ett tredjeland.[180]

Rättsliga grunder

En grundläggande förutsättning för att en myndighet eller ett företag ska ha rätt att behandla personuppgifter är att det finns en rättslig grund för behandlingen. Vilka rättsliga grunder som är godtagbara regleras uttömmande i GDPR. När personuppgifter lämnas ut till ett annat lands myndigheter efter en begäran enligt det landets lagstiftning är det främst fyra rättsliga grunder som skulle kunna komma i fråga.

För det första kan behandlingen vara nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige (artikel 6.1 c), för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning (artikel 6.1 e). En rättslig förpliktelse, uppgift av allmänt intresse eller myndighetsutövning måste vara fastställd i enlighet med unionsrätten eller nationell rätt för att kunna utgöra en laglig rättslig grund.[181] Europeiska dataskyddsstyrelsen m.fl. menar att så länge förfarandet enligt CLOUD Act inte erkänts genom en internationell överenskommelse mellan EU och USA kan de rättsliga grunderna rättslig förpliktelse, uppgift av allmänt intresse eller myndighetsutövning inte tillämpas när en tjänsteleverantör lämnar ut personuppgifter i enlighet med en sådan begäran.[182]

För det andra kan behandlingen vara nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd för personuppgifterna (artikel 6.1 f). Det ska således göras en intresseavvägning mellan den personuppgiftsansvariges och den registrerades intressen. Europeiska dataskyddsstyrelsen m.fl. menar att den personuppgiftsansvariges intresse här skulle kunna bestå i att inte utsättas för rättsliga sanktioner från amerikanska myndigheter för att inte ha hörsammat en begäran om utlämnande. I avsaknad av ett internationellt avtal som stödjer ett utlämnade i enlighet med CLOUD Act menar Europeiska dataskyddsstyrelsen m.fl. dock att överföringen skulle göras utan det skydd som ett sådant avtal ger för bl.a. den registrerades rätt till

---

[179] Se artikel 5 i GDPR.

[180] Se artikel 44 i GDPR. Se även *EPDB-EDPS, Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection*, 2019-07-10, Annex s. 3–4

[181] Se artikel 6.3 i GDPR. I 2 kap. 1 och 2 §§ lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning finns bestämmelser som förtydligar att detta krav för svensk del innebär att den rättsliga förpliktelsen eller uppgiften av allmänt intresse ska följa av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning för att kunna utgöra en godtagbar rättslig grund.

[182] EPDB-EDPS *Joint Response to the LIBE Committee*, Annex s. 5–6

ett effektivt rättsmedel (jfr artikel 47 i stadgan). Europeiska dataskyddsstyrelsen m.fl. påpekar också att en begäran i enlighet med CLOUD Act till sin natur är sådan att det är praktiskt omöjligt för den personuppgiftsansvarige att göra en korrekt utvärdering av alla omständigheter och de konsekvenser för den registrerade som ett utlämnande kan medföra. Mot den bakgrunden bedömer Europeiska dataskydds-styrelsen m.fl. att den registrerades intresse av att personuppgifterna inte lämnas ut bör väga tyngre än den personuppgiftsansvariges intresse av att lämna ut uppgifterna i de fall en begäran om utlämnande riktas mot en tjänsteleverantör i enlighet med CLOUD Act.

Slutligen kan behandlingen vara nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person (artikel 6.1 d). Av skälen till GDPR framgår att en personuppgiftsbehandling endast får stödja sig på denna rättsliga grund om behandlingen inte uppenbart kan ha en annan grund.[183] Eftersom den personuppgiftsbehandling som sker vid utlämnande av personuppgifter i enlighet med CLOUD Act i stället skulle kunna ske i enlighet med den fastställda proceduren i ingångna avtal om ömsesidig rättslig hjälp (MLAT), menar Europeiska dataskyddsstyrelsen m.fl. att ett sådant utlämnande inte kan anses nödvändigt för att skydda någon annan fysisk persons intressen än den registrerades. Europeiska dataskyddsstyrelsen m.fl. utesluter dock inte att det under exceptionella omständigheter kan förekomma att en överföring enligt CLOUD Act kan vara nödvändig för att skydda den registrerades intressen. Som exempel nämns att person-uppgifterna behövs i en utredning gällande bortförda barn. Det noteras dock att en sådan behandling samtidigt måste uppfylla de krav för överföring till tredjeland som ställs upp i artikel 49.1 f (se nedan).[184]

Överföring av personuppgifter till tredjeland

Huvudregeln i GDPR är att en överföring eller ett utlämnande av personuppgifter som har sin grund i ett domstolsbeslut eller beslut från myndigheter i ett tredjeland får genomföras endast om beslutet grundar sig på en internationell överenskommelse som gäller mellan det begärande tredjelandet och unionen eller en medlemsstat, t.ex. en MLAT (artikel 48). Som EU-kommissionen har konstaterat framgår det klart av denna bestämmelse att ett domstolsbeslut från tredjeland inte i sig innebär att en överföring av personuppgifter är laglig enligt GDPR.[185] Europeiska dataskydds-styrelsen har i sina riktlinjer vidare uttalat att i de situationer där det finns en MLAT eller liknande, bör ett företag inom EU generellt avslå direkta förfrågningar om utlämnande och hänvisa tredjelandsmyndigheten till befintligt avtal.[186]

Överföring av personuppgifter får vidare ske om kommissionen har fattat beslut om att det tredjelandet säkerställer en adekvat skyddsnivå. Om ett sådant beslut inte fattats får personuppgifter föras över till ett tredjeland efter att vissa angivna lämpliga skyddsåtgärder vidtagits och under förutsättning att lagstadgade rättigheter och effektiva rättsmedel finns tillgängliga för de registrerade (artiklarna 45, 46 och 47). Kommissionen har antagit hållningen att ingen av dessa förutsättningar troligen

---

[183] Se skäl 46 till GDPR.

[184] EPDB-EDPS, *Joint Response to the LIBE Committee*, Annex s. 7–8

[185] Europeiska kommissionen, *Brief of the European Commission on behalf of the European Union as amicus curiae in support of neither Party in the case United States v. Microsoft Corp*. Se också Europeiska dataskyddsstyrelsen, *Riktlinjer 2/2018 för undantagen i artikel 49 enligt förordning 2016/679*, antagna den 25 maj 2018, s. 5.

[186] Europeiska dataskyddsstyrelsen, *Riktlinjer 2/2018*, s. 5

är uppfyllda i en situation där myndigheterna i ett tredjeland begär tillgång till uppgifter som lagras inom EU.[187]

Utifrån de bedömningar Europeiska dataskyddsstyrelsen och kommissionen gjort gällande artiklarna 45-48 i GDPR måste således någon av de undantagssituationer som framgår av artikel 49.1 föreligga för att ett utlämnande av personuppgifter i enlighet med ett tredjelands lagstiftning ska vara lagligt enligt GDPR.[188] I en sådan situation är det främst fyra av dessa undantag som kan komma i fråga.

Det första undantaget tar sikte på överföringar som är nödvändiga av viktiga skäl som rör allmänintresset (artikel 49.1 d). Detta allmänintresse ska vara erkänt i unionsrätten eller i den nationella rätt som den personuppgiftsansvarige omfattas av.[189] Europeiska dataskyddsstyrelsen m.fl. menar att hänsyn inte kan tas till ett tredjelands intresse i detta fall. Det är inte heller tillräckligt att det tredjelandets intresse, t.ex. av att vidta en viss utredning, i abstrakt mening också ligger i EU:s eller i en medlemsstats intresse.[190]

Det andra undantag som skulle kunna tillämpas är undantaget för överföringar som är nödvändiga för att kunna fastställa, göra gällande eller försvara rättsliga anspråk (artikel 49.1 e). Europeiska dataskyddsstyrelsen m.fl. understryker att detta undantag kräver en nära koppling mellan överföringen av uppgifter och ett specifikt förfarande och att undantaget inte kan användas för att motivera överföring av personuppgifter endast på grundval av att en process eller ett formellt förfarande kan komma att äga rum i framtiden.[191]

Det tredje undantag som kan komma i fråga är att överföringen är nödvändig för att skydda den registrerades eller andra personers grundläggande intressen, när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke (artikel 49.1 f). Europeiska dataskyddsstyrelsen m.fl. menar att, precis som för den rättsliga grunden i artikel 6.1 d, skulle skyddet för den registrerades intresse i exceptionella fall kunna medföra att förutsättningarna för detta undantag är uppfyllda. EDPB m.fl. har också gett uttryck för att kravet på att den registrerade ska vara förhindrad att lämna sitt samtycke kan inkludera situationer där det är den registrerade som utgör ett omedelbart hot mot andra personers liv eller fysiska integritet. En förutsättning uppges dock vara att det finns tillräcklig information för att fastställa rättsenligheten. Europeiska dataskyddsstyrelsen betonar dock att andra personers intressen inte kan användas som rättslig grund för en överföring till tredjeland om det finns andra rättsliga grunder som kan användas i stället, t.ex. när det finns en överenskommen MLAT-procedur.[192]

Om ingen av de nyss nämnda undantagen är tillämpliga, finns ett sista tillämpbart undantag i artikel 49.1 andra stycket i GDPR. Enligt detta undantag får en överföring till ett tredjeland äga rum endast om den är nödvändig för ändamål som rör den

---

[187] Europeiska kommissionen, *Brief of the European Commission*

[188] Om kommissionen inte fattat något beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder inte vidtagits, får överföring till ett tredje land endast ske om någon av undantagssituationerna i artikel 49.1 i GDPR föreligger.

[189] Se artikel 49.4 i GDPR.

[190] EPDB-EDPS, *Joint Response to the LIBE Committee*, Annex s. 6

[191] EPDB-EDPS, *Joint Response to the LIBE Committee,* Annex s. 6–7 och Europeiska dataskyddsstyrelsen, *Riktlinjer 2/2018*, s. 11–12

[192] EPDB-EDPS, *Joint Response to the LIBE Committee*, Annex s. 7

personuppgiftsansvariges tvingande berättigade intressen och den registrerades intressen eller rättigheter och friheter inte väger tyngre. Det ska således göras en avvägning, där dessa två intressen ställs mot varandra. Tillämpningsområdet för detta undantag är särskilt snävt och undantaget innehåller ett antal kriterier som ska vara uppfyllda för att det ska få tillämpas. Den personuppgiftsansvarige ska exempelvis ha bedömt samtliga omständigheter kring överföringen och utifrån denna bedömning vidtagit lämpliga skyddsåtgärder för personuppgifterna. Den personuppgiftsansvarige har också en skyldighet att informera både tillsynsmyndigheten och den registrerade.

EU-kommissionen menar att den personuppgiftsansvariges intresse av att inte bli föremål för rättsliga sanktioner i ett tredjeland skulle kunna vara ett sådant berättigat intresse som avses i detta sista undantag.[193] Europeiska dataskyddsstyrelsen m.fl. konstaterar dock att de krav som ska vara uppfyllda vad gäller detta undantag är mycket högre än de som gäller för att använda sig av den rättsliga grunden intresseavvägning artikel 6.1 f i GDPR. Europeiska dataskyddsstyrelsen m.fl. pekar också på flera svårigheter med att använda detta undantag vid en begäran enligt CLOUD Act. För det första är det, precis som när det gäller den rättsliga grunden intresseavvägning, svårt att utföra en korrekt utvärdering av alla omständigheter och möjliga konsekvenser för den registrerade. För det andra är en begäran om utlämnande i enlighet med CLOUD Act ofta förenad med yppandeförbud för att inte äventyra brottsutredningen. Detta medför svårigheter för den personuppgiftsansvarige att informera tillsynsmyndigheten och den registrerade. För det tredje kommer det inte att vara praktiskt möjligt för den personuppgiftsansvarige att vidta lämpliga skyddsåtgärder för överföringen. Mot den bakgrunden bedömer Europeiska dataskyddsstyrelsen m.fl. att undantaget i artikel 49.1 andra stycket inte kan tillämpas för att lagligen föra över personuppgifter till amerikanska myndigheter efter en begäran i enlighet med CLOUD Act.[194]

Konsekvensen av konflikten mellan CLOUD Act och GDPR för svenska myndigheter

Enligt den bedömning som Europeiska dataskyddsstyrelsen m.fl. gjort finns det således för närvarande rättslig grund för ett överförande till tredjeland i enlighet med CLOUD Act endast i undantagsfall, i syfte att skydda den registrerades intressen. Detsamma gäller förutsättningarna för lagenlig överföring till ett tredjeland enligt bestämmelserna i kapitel V i GDPR.

En personuppgiftsansvarig eller ett personuppgiftsbiträde som lämnar ut personuppgifter till ett tredjelands myndigheter utan att det finns en rättslig grund för det enligt GDPR riskerar ytterst att drabbas av ansenliga administrativa sanktionsavgifter.[195] Detsamma gäller när personuppgifter förs över till tredjeland utan att någon av förutsättningarna i avsnitt V i GDPR är uppfyllda. Den som hörsammar en begäran i enlighet med CLOUD Act riskerar således sanktioner i enlighet med EU-rätten. Skulle en sådan begäran inte hörsammas finns risk för rättsliga sanktioner i

---

[193] Europeiska kommissionen, *Brief of the European Commission*

[194] EPDB-EDPS, *Joint Response to the LIBE Committee*, Annex s. 7

[195] Se artiklarna 44 och 48 jämförda med artikel 83.5 c i GDPR. Sanktionsavgifterna kan uppgå som mest till 20 miljoner euro eller 4 procent av ett företags globala årsomsättning.

USA. I praktiken innebär detta att tjänsteleverantörerna riskerar att utsättas för en konflikt mellan EU-rätten och amerikansk lag.[196]

En svensk myndighet är troligtvis inte personuppgiftsansvarig för den personuppgiftsbehandling som sker när ett anlitat personuppgiftsbiträde, t.ex. en tjänsteleverantör, lämnar ut uppgifter till ett tredjeland i strid med avtalet. Som personuppgiftsansvarig får myndigheten dock endast anlita biträden som ger tillräckliga garantier för att den registrerades rättigheter skyddas och för att behandlingen genomförs i enlighet med GDPR. Brister i den hanteringen kan resultera i sanktionsavgifter.[197] Den myndighet som vill använda sig av molntjänster måste därmed se till att det inte anlitas en tjänsteleverantör som kan komma att bryta mot GDPR eller mot personuppgiftsbiträdesavtalet.

[196] EPDB-EDPS, *Joint Response to the LIBE Committee*, Annex s. 2

[197] Se artiklarna 28.1 och 83.4 a i GDPR. För en myndighet kan sådana avgifter uppgå till maximalt 10 miljoner euro.

Bilaga 4 Exempel på tjänsteleverantörers utlämnande av kunddata till brotts-bekämpande myndigheter

Flera leverantörer publicerar regelbundet rapporter om förfrågningar från brotts-bekämpande myndigheter avseende data. Det är oklart hur kompletta rapporterna är och eftersom olika aktörer publicerar olika information på olika sätt är de inte jämförbara. Syftet med detta kapitel är att utifrån publikt publicerad information få en övergripande bild av om data lämnas ut av leverantörer och vilken information som finns tillgänglig om utlämnande från stora leverantörer.

Microsoft publicerar en rapport en gång i halvåret. En hel del av förfrågningarna rör privatpersoners konton, men Microsoft beskriver också förfrågningar om icke konsumentkonton. Microsoft angav att under andra halvan av 2018 inkom 61 förfrågningar globalt avseende konton associerade med molnkunder med mer än 50 användarkonton. I 22 ärenden lämnade Microsoft efter prövning ut data. Av dessa 22 ärenden lämnades innehåll ut i 15 ärenden och i sju ärenden lämnades metadata ut. Av de 15 ärenden där innehåll lämnades ut var åtta associerade med amerikansk rättsbekämpande myndigheter. Under samma period begärde amerikanska rättsbekämpande myndigheter ut data i 36 ärenden som avsåg kunder med mer än 50 användare. Av dessa krav avsåg ett data som lagrades utanför USA.[198]

AWS publicerar inte data separerat på privatpersoners konton och organisationers tjänster. AWS publicerar bland annat antal förfrågningar specifikt avseende deras molntjänst AWS. Om man exkluderar förfrågningar rörande rikets säkerhet, som är helt hemlighetsstämplade, hade 271 förfrågningar inkommit 2018. I dessa fall lämnades data ut i 200 fall.[199]

Google publicerar kontinuerliga rapporter om begäran och utlämnande av data till myndigheter. De beskriver också att de vill vara öppna med informationen, eftersom de vill rikta uppmärksamheten på den stora omfattningen av begäranden samt på de lagar och juridiska processer som påverkar åtkomsten till information online.

Google rapporterar också andelen ärenden där begäran resulterar i ett utlämnande. Sammanlagt uppger Google att 2011-2018 lämnades data ut till brottsbekämpande myndigheter i 375 604 fall. Antalet begäranden ökar och i ungefär 75 % av ärendena lämnas data ut.[200]

---

[198] Microsoft, *Law Enforcement Requests Report*

[199] AWS, *Information Request Report*

[200] Google, *Begäran om användarinformation*

Bilaga 5 Säkerhetsskyddet

Bestämmelserna säkerhetsskydd utgör en viktig del av skyddet för samhällsbärande funktioner. I denna bilaga redogör vi i korthet för det skydd för säkerhetskänslig verksamhet som framgår av säkerhetsskyddslagen (2018:585).

Säkerhetskänslig verksamhet samt informations- och personalsäkerhet

Säkerhetsskyddslagen gäller för den som bedriver säkerhetskänslig verksamhet, vilket bl.a. innefattar verksamhet som är av betydelse för Sveriges säkerhet.[201] Den som bedriver säkerhetskänslig verksamhet ska genom förebyggande arbete skydda denna mot spionerі, sabotage, terroristbrott och vissa andra hot.[202] Säkerhetskänsliga verksamheter identifieras utifrån vilken skada som uppstår för Sveriges säkerhet om en angripare inhämtar information om verksamheten, förstör information eller på annat sätt hindrar att verksamheten kan bedrivas.[203] Säkerhetsskyddsarbetet ska utgå från en säkerhetsskyddsanalys, som syftar till att identifiera vilken verksamhet och vilka informationstillgångar som omfattas av säkerhetsskyddslagen och om skyddet för dessa är tillräckligt.[204] Kraven på hanteringen av säkerhetsskyddsklassificerade uppgifter ökar med klassificeringsnivån.

Säkerhetskänslig verksamhet bedrivs bl.a. av svenska myndigheter, t.ex. Försäkringskassan. I säkerhetsskyddslagen finns bestämmelser om vilka säkerhetsskyddsåtgärder som ska vidtas för säkerhetskänslig verksamhet. Dessa åtgärder består bl.a. av informations- och personalsäkerhet.[205]

Informationssäkerhet handlar om att skydda information, oavsett var den finns, på ett sätt så att den inte kan delas med eller ändras av obehöriga personer. Det handlar också om att se till att information finns till hands när den behövs. Allt i syfte att undvika de stora negativa konsekvenserna för en verksamhet som sådana situationer kan innebära.[206]

En anställning eller annat deltagande i säkerhetskänslig verksamhet placeras vanligen i säkerhetsklass, utifrån vilken typ av uppgifter personen kommer att få del av och i vilken utsträckning detta kommer att ske.[207] Vid en anställning i stat, kommun eller region som är placerad i säkerhetsklass 1 eller 2 finns krav på svenskt medborgarskap. Detta krav gäller dock inte för annat deltagande i säkerhetskänslig verksamhet som bedrivs av stat, kommun eller region.[208] Syftet med personalsäkerhet är att förebygga att personer som inte är pålitliga från säkerhets-

---

[201] 1 kap. 1 § säkerhetsskyddslagen

[202] 1 kap. 2 § säkerhetsskyddslagen

[203] 2 kap. 5 § säkerhetsskyddslagen. De fyra säkerhetsskyddsklasserna är 1) kvalificerat hemlig om den skada som kan uppstå är synnerligen allvarlig, 2) hemlig vid en allvarlig skada, 3) konfidentiell vid en inte obetydlig skada och 4) begränsat hemlig vid endast ringa skada.

[204] 2 kap. 1 § säkerhetsskyddslagen

[205] Därutöver ingår även fysisk säkerhet. Se 2 kap. 2-4 §§ säkerhetsskyddslagen.

[206] 2 kap. 2 § säkerhetsskyddslagen. Se även Säkerhetspolisen, Informationssäkerhet.

[207] 3 kap. 5–10 §§ säkerhetsskyddslagen

[208] 3 kap. 11 § säkerhetsskyddslagen

synpunkt deltar i en verksamhet där de kan få tillgång till säkerhetsskydds-klassificerade uppgifter eller i en verksamhet som av någon annan anledning är säkerhetskänslig. Personalsäkerheten ska också säkerställa att de personer som deltar i säkerhetskänsligverksamhet har tillräcklig kunskap om säkerhetsskydd. Den som ska anställa eller anlita en person i säkerhetskänslig verksamhet ska göra en säkerhetsprövning innan personen deltar i verksamheten. Detta gäller oavsett om deltagandet ska ske genom anställning eller på något annat sätt. Syftet med prövningen är att klarlägga om personen kan antas vara lojal med de intressen som ska skyddas och i övrigt pålitlig ur säkerhetssynpunkt. Ett annat syfte är att utreda eventuella sårbarheter som skulle kunna göra att personen hamnar i en utsatt situation och blir sårbar för yttre påtryckningar.[209]

En säkerhetsprövning av personer som ska delta i säkerhetskänslig verksamhet ska göras av den som beslutar om anställning eller annat deltagande i den säkerhets-känsliga verksamheten. Om en myndighet har det bestämmande inflytandet över den prövades lämplighet att delta i säkerhetskänslig verksamhet hos en enskild verksamhetsutövare, är det i stället myndigheten som gör den slutliga bedömningen.[210] Säkerhetsprövningen består normalt sett av grundutredning, registerkontroll och utbildning i säkerhetsskydd. Under grundutredningen kartläggs personens personliga förhållanden i den del som har betydelse för säkerhets-prövningen. Detta görs bl.a. genom en säkerhetsprövningsintervju, som är ett av de viktigaste verktygen för att inhämta underlag för denna bedömning. Därtill kan betyg, intyg och referenser som är av relevans hämtas in och bedömas. Även övriga uppgifter, t.ex. information från öppna källor, som sociala medier och internet, kan bidra till att skapa en mer komplett bild av personen.[211] Efter en grundutredning med tillfredsställande resultat vad gäller lojalitet, pålitlighet och sårbarhet ska säkerhetsprövningen normalt kompletteras med en framställan om registerkontroll till Säkerhetspolisen, om tjänsten är inplacerad i säkerhetsklass.[212] Register-kontrollen omfattar uppgifter som hämtas från belastningsregistret, misstanke-registret samt uppgifter som behandlas med stöd av lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område.[213]

När det gäller personer som har haft hemvist i ett annat land har dock Säkerhets-polisen begränsade möjligheter att genomföra kvalitativa registerkontroller. Säkerhetspolisen menar att verksamhetsutövaren i dessa fall måste ta höjd för detta i säkerhetsprövningen, t.ex. genom att fördjupa bakgrundskontrollen. Det bör enligt Säkerhetspolisen ställas högre krav på inhämtning av referenser för säkerhets-prövningen av personer som saknar hemvist i Sverige, då möjligheterna att utnyttja svenska kontrollinstrument är begränsade i utlandet.[214]

---

[209] 2 kap. 4 § och 3 kap. 1–2 §§ säkerhetsskyddslagen. Se även Säkerhetspolisen, Personalsäkerhet

[210] 3 kap. 4 § andra stycket säkerhetsskyddslagen och 5 kap. 4 § säkerhetsskyddsförordningen. Se även Säkerhetspolisen, *Vägledning i säkerhetsskydd – personalsäkerhet,* juni 2019, s. 18.

[211] 3 kap. 3 och 4 §§ säkerhetsskyddslagen (2018:585), 5 kap. 2 § säkerhetsskyddsförordningen (2018:658) och 6 kap. 4 § Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd. Se även Säkerhetspolisen, *Vägledning i säkerhetsskydd*, s. 11–12

[212] 3 kap. 14 § säkerhetsskyddslagen (2018:585)

[213] 3 kap. 13 § säkerhetsskyddslagen

[214] Säkerhetspolisen, *Vägledning i säkerhetsskydd*, s. 26

Säkerhetsskyddad upphandling

Säkerhetskänslig verksamhet ska ha samma skydd oavsett vilken aktör som bedriver den. En myndighet ska alltså kräva samma nivå på säkerhetsskyddet hos leverantörer som den ställer i sin egen verksamhet.[215] Säkerhetsskyddad upphandling är den process där den upphandlande myndigheten analyserar vilka skyddsvärden som finns i upphandlingen. Statliga myndigheter, kommuner och landsting som gör vissa typer av upphandlingar med koppling till säkerhetskänslig verksamhet ska teckna ett säkerhetsskyddsavtal med anbudsgivaren eller leverantören där det framgår hur denne ska uppfylla kraven på säkerhetsskydd. Ett sådant avtal ska också tecknas med eventuella underleverantörer. Myndigheten ska även kontrollera och följa upp att leverantörerna faktiskt vidtagit de åtgärder som myndigheten ställt krav på.[216] Som en av riskerna vid upphandling i säkerhetskänslig verksamhet har Säkerhetspolisen pekat på att de krav som ställs i säkerhetsskyddsavtalet ibland är så allmänt hållna att de är svåra att följa upp.[217]

Säkerhetsskyddsavtalet utgör också en grund för att besluta om vilka anställningar och annat deltagande hos leverantören som ska placeras i säkerhetsklass. När en myndighet tecknar ett säkerhetsskyddsavtal med en leverantör ska detta meddelas Säkerhetspolisen. Syftet är att Säkerhetspolisen ska kunna genomföra register-kontroll på personer som kommer att ha säkerhetsklassade befattningar kopplade till avtalet.[218]

---

[215] Säkerhetspolisen, *Säkerhetsskydd vid upphandlingar och affärsavtal*

[216] 2 kap. 6 § säkerhetsskyddslagen. Bestämmelsen avser upphandlingar och avtal om varor, tjänster eller byggentreprenader om det i upphandlingen förekommer säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre, eller om upphandlingen i övrigt avser eller ger leverantören tillgång till säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet.

[217] Säkerhetspolisen, *Årsbok 2017*, s. 56

[218] Säkerhetspolisen, *Säkerhetsskydd vid upphandlingar och affärsavtal*

Bilaga 6 Klassificeringen av samhällsviktig verksamhet – exemplet Transportstyrelsen

Transportstyrelsen arbetar för att uppnå god tillgänglighet, hög kvalitet, säkra och miljöanpassade transporter inom järnväg, luftfart, sjöfart och väg. Transportstyrelsen tar fram regler, ger tillstånd och följer upp hur de efterlevs. Med hjälp av register arbetar myndigheten med avgifter, tillstånd och ägarbyten.

År 2017 genomförde Transportstyrelsen en säkerhetsanalys för att identifiera skyddsvärd verksamhet, potentiella antagonister, konsekvenser vid röjning eller förstörning samt åtgärder för att eliminera sårbarheter. Säkerhetsanalysen finns inte publikt tillgänglig men vissa generella slutsatser har publicerats i en av regeringen begärd utredning.[219]

Transportstyrelsen hanterar enligt säkerhetsanalysen mycket stora mängder information och data. En mycket liten del av informationen är hemlig och en liten andel information omfattas av sekretess. Den stora mängden information är dock att betraktas som offentlig och kan begäras ut av allmänheten.

En annan problematik är att den totala informationsmängden i sig är en skyddsvärd tillgång. Detta eftersom högupplösta grunddata med sin detaljrikedom ger en alltför heltäckande bild av informationsinnehållet sett till olika säkerhetsperspektiv. Någon som har tillgång till helheten kan genom att analysera olika uppgifter upptäcka avvikelser och på detta sätt genom slutledning få fram hemlig information. Med en oinskränkt tillgång till stora informationsmängder följer i regel risker för åtgärder och analyser som av säkerhetsskäl inte bör få förekomma. Även avsaknad av information som borde ha funnits kan utgöra en risk.[220]

I utredningen av Transportstyrelsens outsourcing 2017 konstateras att av säkerhetsskäl hade Transportstyrelsen strategin att så få personer som möjligt skulle ha kännedom om vilka typer av uppgifter myndigheten hanterade. Hela informationsmängden ska därför betraktas som säkerhetskänslig. Eftersom de uppgifter som omfattas av sekretess och hemligstämpling finns spridd i den övriga informationen blir det problematiskt att utforma it-stöd där vissa delar är att betrakta som icke samhällsviktiga medan andra delar inte är det.[221]

---

[219] Transportstyrelsen, *Kartläggning av hanteringen av vissa uppgifter*

[220] Till exempel Polismyndigheten gör vid behov slagningar mot Transportstyrelsens register.

[221] SOU 2018:6, *Granskning av Transportstyrelsens upphandling av it-drift*, s. 76–77, 84, 100, 220 och 223

Bilaga 7 Kryptering för att skydda uppgifter från röjande

Att kryptera innebär är att information görs svårläslig för alla som inte ska kunna läsa den. För att göra informationen läslig igen krävs dekryptering. Det betyder att den som krypterar informationen och den som ska läsa informationen ska ha tillgång till den nyckel som behövs för att dekryptera informationen. Inte minst militära och politiska organisationer har en lång erfarenhet av kryptering. Kryptering görs för att obehöriga inte ska få tillgång till informationen.

Så länge kryptering funnits har obehöriga dock försökt lista ut krypteringsnyckeln för att få tillgång till informationen.

I och med införandet av datorer har kryptering och dekryptering automatiserats och krypton behöver vara allt mer komplexa för att inte obehöriga ska kunna bryta dem.

Kryptering kan i princip vara tillämpbart vid två principiella situationer; när information lagras och när information transporteras. Eftersom utmaningarna är olika för lagring och transport är det viktigt att kunna säkerställa vilken form av kryptering som avses.

Det är också viktigt att betänka att data i praktiken inte kan bearbetas när den är krypterad. För att kunna bearbeta data behöver den dekrypteras först. Det innebär att om bearbetning görs i en funktion hos leverantören behöver leverantören ha möjlighet att dekryptera.

Enligt 3 kap. 5 § säkerhetsskyddsförordningen (2018:658) ska alla verksamheter, offentliga och privata, som hanterar säkerhetsskyddsklassificerade uppgifter som ska kommuniceras till ett informationssystem utanför verksamhetsutövarens kontroll, skydda uppgifterna med hjälp av kryptografiska funktioner som har godkänts av Försvarsmakten[222]. Försvarets kryptografiska funktioner är inte avsedda eller lämpliga för all typ av information och verksamhet.

Leverantörer kan erbjuda sina kunder kryptering som en del av tjänsteutbudet. Vilka tjänster som erbjuds och vilket skydd de erbjuder varierar och detta ska bara ses som exempel. Det är dock värt att notera att många av de tjänster som erbjuds av de stora molntjänsteleverantörerna inte är godkända av Försvarsmakten.

Microsoft erbjuder tre grundtjänster för kryptering i sina molntjänster; Customer key, Bring your own key och Hold your own key. AWS erbjuder också krypteringstjänster där både kunden och AWS håller nyckeln och exemplet nedan utgör bara ett exempel på tillämpning.[223]

---

[222] Försvarsmakten, *Försvarsmaktens föreskrifter om signalskyddstjänsten och Försvarsmakten, Godkända kryptoapparater september 2019*

[223] AWS, *Protection Data using encryption*

Customer key/service encryption

Microsoft erbjuder tjänsten för Sharepoint Online, Onedrive Business och Exchange Online. Tjänsten innebär ett skydd mot fysisk tillgång till data om till exempel en obehörig får tillgång till en hårddisk.

Krypteringsmetoden skyddar inte mot behörigs tillgång till data. Data krypterad med denna metod kan tillgås av behörig tekniker hos leverantören och kan lämnas ut till en utländsk myndighet enligt gällande rättsordning.[224]

Bring your own key

Microsoft erbjuder tjänsten för kryptering av enskilda dokument och kan därför vara tillämpbar för enskilda e-postmeddelanden eller dokument.

Ägaren kan välja att kryptera dokumenten. Microsoft har dock tillgång till nyckeln för att kunna läsa och indexera data och skyddar dokument för obehörig tillgång till dokumentet.

Data krypterad med denna metod kan tillgängliggöras av behörig tekniker hos leverantör och kan lämnas ut till utländsk myndighet enligt gällande rättsordning.[225]

Hold your own key

Tjänsten erbjuds av Microsoft för kryptering av enskilda dokument och kan därför vara tillämpbar för enskilda e-postmeddelanden eller dokument. Ägaren kan välja att kryptera dokumenten. Kunden äger dock hela kedjan av nycklar, vilket innebär att leverantören inte har tillgång till nyckel för dekryptering.

Denna avsaknad av tillgång innebär dock att användbarheten av it-tjänsten blir mycket begränsad. Ett exempel är att användaren inte kan använda sökfunktioner och samverkan med andra externa parter blir mycket begränsad.

Denna metod skulle, givet att en utländsk myndighet inte ställer krav på tillgång till krypteringsnyckel, kunna förhindra tillgång av behörig tekniker hos leverantören och data kan inte lämnas ut dekrypterat till utländsk myndighet enligt gällande rättsordning.

Lösningen skulle dock innebära en försämrad funktionalitet hos användarna i vardaglig användning av t.ex. kontorsprogram. Dels för att vissa funktioner inte skulle vara tillgängliga alls, dels för att prestandan skulle påverkas negativt.[226]

---

[224] Microsoft, *Service encryption with Customer Key for Office 365 FAQ*

[225] Microsoft, *Prisnivåer och begränsningar för BYOK*

[226] Microsoft, *Håll din egen nyckel skydd (HYOK) för Azure Information Protection*

Utländska myndigheters tillgång till krypteringsnycklar

Lagar om utlämning av krypteringsnycklar förekommer i ett antal länder. Europarådet föreslog 2013 att denna möjlighet skulle införas inom EU.[227] I Sverige saknas för närvarande sådan lagstiftning. Den 24 oktober 2019 beslutade regeringen dock lagrådsremissen Hemlig dataavläsning. Där föreslås att de brottsbekämpande myndigheterna ska få möjlighet att använda bl.a. dekryptering som hemligt tvångsmedel vid misstankar om allvarlig brottslighet.[228]

I Norden var Danmark det första land som införde lagstiftning som möjliggjorde hemlig dataavläsning 2002. Motsvarande lagstiftning har sedan införts även i Finland och Norge och lagstiftningen inkluderar möjlighet till dekryptering.[229]

En studie som genomfördes på uppdrag av EU-parlamentet 2017 visar att metoder för hemlig dataavläsning används i de jämförda EU-staterna, i vissa fall med uttryckligt lagstöd och i andra fall utan sådant. I de stater där det inte finns explicit lagstiftning pågår för närvarande lagstiftningsarbete.[230]

I Europaparlamentets utredning analyserades även tre utomeuropeiska länder. Australien konstaterades sakna explicit lagstiftning men utredningen kunde utesluta att hemliga tvångsmedel används med stöd av annan äldre lagstiftning.[231] Israel konstaterades ha ett tydligare lagutrymme och ger bland annat utrymme för dekryptering.[232]

Eftersom exemplet som används här beskriver den amerikanska lagstiftningen används även det aktuella rättsläget i USA för att exemplifiera även utländska myndigheters möjligheter att få tillgång till krypteringsnycklar mer i detalj. Utredningen som genomfördes 2017 på uppdrag av Europaparlamentet belyste också hur hemliga tvångsmedel tillämpas av amerikanska brottsbekämpande myndigheter.[233]

Den amerikanska konstitutionens femte artikel gör gällande att en person inte ska tvingas att framföra bevis som talar emot den egna saken och detta kan ses som ett hinder för att kräva tillgång till krypteringsnycklar.[234] Det finns dock rättsfall där krypteringsnycklar och lösenord utlämnats. Det första fallet var *In re Boucher* där den åtalade initialt hade lovat tillgång till den egna hårddisken men då delar av hårddisken var krypterad kunde inte all information tillgängliggöras. Åklagaren framförde att de inte avkrävde den åtalade dennes lösenord utan att innehållet skulle tillgängliggöras åtalsjuryn och att det därför inte skulle bryta mot den femte artikeln

---

[227] Utredningen om it-brottskonventionen, *Europarådets konvention om it-relaterad brottslighet* (SOU 2013:39), s. 280ff

[228] Justitiedepartementet, Lagrådsremiss, *Hemlig dataavlyssning*, 2019-10-24, s. 1 och 57

[229] Utredningen om hemlig dataavläsning, *Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet* (SOU 2017:89), s. 121–147

[230] Europaparlamentet, *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*, (PE 583.137), s. 72–110

[231] PE 583.137 s. 111–116

[232] PE 583.137 s. 117–120

[233] PE 583.137 s. 121–128

[234] Corey Varma, *Encryption vs. Fifth Amendment*

i konstitutionen och domaren biföll denna begäran eftersom den åtalade redan hade erbjudit sig att ge tillgång till hårddisken.[235]

I ett annat rättsfall bedömdes femte artikeln vara tillämplig och krypteringsnycklar lämnades inte ut. I det fallet beslagtog amerikanska FBI ett antal datorer och hårddiskar men kunde inte avkryptera hårddiskarna. Electronic Frontier Foundation (EFF) förde mannens talan och den 11e US Circuit court biföll EFFs begäran och hävdade att mannens krypteringsnycklar var skyddade av femte artikeln.[236]

Begäran om krypteringsnycklar via en leverantör har bland annat behandlats i en rapport från Massachusetts institute of technology (MIT). I rapporten beskrivs hur det redan 1997 fanns ett förslag, Clipper Chip, som krävde att alla starka krypteringssystem skulle finnas hos en betrodd part och skulle efter en juridisk process kunna utlämnas till brottskämpande myndigheter. Kostnaderna och riskerna bedömdes till sist bli för stora och projektet övergavs.[237]

I rapporten analyseras de 2015 liggande förslagen på att ge amerikanska rättsbekämpande myndigheterna möjligheten att efter beslutad rättsprocess få tillgång till krypteringsnycklar. Rapporten gör gällande att detta skulle få till följd att de funktioner som nu införs för att göra Internet säkrare troligen skulle få mer begränsad spridning eftersom förtroendet för skyddet skulle skadas. Rapporten pekar också på att om leverantörer ska ha en skyldighet att kunna tillhandahålla krypteringsnycklar skulle det i praktiken leda till mer komplexa system som i sig i regel leder till nya risker. Slutligen bedöms funktioner för att kunna dekryptera som en måltavla i sig för antagonister, vilket kan leda till ytterligare sårbarheter.[238]

Sammantaget är det rättsliga läget för amerikanska myndigheters möjligheter att efter juridisk process få tillgång till krypteringsnycklar oklart och beroende av bedömningen i det individuella fallet.

Vad det rättsliga läget skulle vara för en leverantör med säte i ett land men där data lagras fysiskt i ett annat tycks vara oklart, särskilt eftersom reglerna kan variera beroende på eventuella avtal mellan länder och en tjänst kan vara sammansatt av tjänster från olika leverantörer från olika länder. Om en leverantör eller en tjänst blir uppköpt blir rättsläget ännu svårare att bedöma.

---

[235] United States District Court for the District of Vermont. No. 2:06-mj-91, 2009 WL 424718 Feb. 19, 2009. *Memorandum Of Decision In re Grand Jury Subpoena to Sebastien Boucher*

[236] EFF in the United States Court of Appeals for the Eleventh Circuit *Case: 11-12268*

[237] Abelson Harold m.fl., *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications2015* (MIT-CSAIL-TR-2015-026) s. 6.

[238] Abelson Harold m.fl. *Keys Under Doormat* s. 24 ff

Bilaga 8 Leverantörers hantering av telemetridata

Telemetridata är mätdata. Många leverantörer samlar in telemetridata och exemplen nedan utgör bara en illustration.[239]

Enligt Microsoft använder företaget telemetridata för att

- hålla en applikation uppdaterad,
- säkerställa att en applikation är säker, pålitlig och fungerar väl,
- förbättra en applikation genom att Microsoft kan analysera aggregerade användardata,
- personalisera användarupplevelsen och
- skapa förståelse för hur användarna använder och inte använder funktioner.[240]

Microsoft har uppgett att man samlar in bl.a. följande telemetridata avseende Windows.

- Typ av hårdvara,
- vilka applikationer som finns installerade på enheten och hur de används,
- hur väl drivrutiner fungerar och
- användares inställningar.

År 2017 analyserade Dutch Data Protection Authority telemetrisk data i Windows 10.[241] Utredningen visade att även om användaren valde den mest begränsande inställningen skickades känslig data till Microsoft. Även vid användande av den mest tillåtande inställningen skickades mycket känsliga data som besökta webbsidor och innehåll i dokument. Studien visade att data som samlades in från användning av applikationer omfattade känsliga personuppgifter, t.ex. från en applikation för muslimska bönetider och en applikation för gravida. Data som samlades in användes bland annat för att visa anpassade annonser för användaren.[242]

År 2018 lät den nederländska regeringen genomföra en konsekvensbedömning enligt GDPR som bland annat behandlade telemetriska data i Microsoft Office Pro Plus, inklusive fristående Office 2016 och Office 365. Syftet var att underlätta för statliga organ att kartlägga och bedöma riskerna i förhållande till de registrerade vid sådan användning samt att planera adekvata åtgärder för att hantera dem.[243]

---

[239] Telemetridata samlas inte bara in från användare av publika molntjänster och som exemplet visar kan telemetridata även samlas in från tjänster som är installerade hos kunden. Dock ger publika molnbaserade tjänster större möjligheter till hämtande av telemetridata

[240] Microsoft, *Konfigurera diagnostikdata för Windows i din organisation*, 2019

[241] Autoriteit Persoonsgegevens (Dutch DPA), *Summary of Investigation Report Public Version Microsoft Windows 10 Home and Pro*, Augusti 2017. Notera att Windows 10 inte är en publik molntjänst.

[242] Rapporten beskriver inte explicit hur data hanterats och vilka tredje parter som fått tillgång till den, men det går inte att utesluta att data tillgängliggjorts för tredje part för att möjliggöra personaliserade annonser.

[243] Ministry of Justice and Security Strategic Vendor Management Microsoft, *DPIA Office 365 ProPlus version 1905 (June 2019) Data protection impact assessment on the processing of diagnostic data*

Enligt konsekvensbedömningen samlar till exempel Microsoft in uppskattningsvis 25 000 olika typer av händelser om Office 365. Telemetridata skickas krypterad till Microsofts servrar. Microsoft samlar även in telemetriska data avseende operativsystemet Windows 10, men detta är avgränsat till 1 000 händelser. Enligt de svar som Microsoft lämnat under utredningen har ett antal utvecklingsteam global tillgång till data.

Utredningen avseende Office Pro Plus identifierar följande risker med Microsofts åtkomst till dessa uppgifter.

- Det saknas transparens till allmänheten vilken information som Microsoft tar del av eftersom det saknas publikt tillgänglig information. Detta förhindrar en organisation från att göra en riskbedömning.
- Det finns inga möjligheter att styra vilka telemetriska uppgifter som skickas.
- Microsoft hämtar och lagrar potentiellt känsliga data, både i form av metadata[244] och innehåll[245], vilket det saknas lagligt stöd för.
- Microsoft agerar som personuppgiftsbiträde istället för gemensamt personuppgiftsansvarig, vilket de borde göra enligt artikel 26 i GDPR.
- Det saknas kontroll över underprocesser och faktisk hantering.
- Det saknas begränsning för i vilka syften data hämtas ut och nya händelser läggs till vid exempelvis uppdateringar.
- Överföring görs till länder utanför EU.
- Det är oklart hur länge data sparas och det saknas möjligheter för kund att ta bort data. [246]

Nederländernas regering har under 2019 förhandlat fram ett tilläggsavtal med Microsoft, som justerar villkoren för Microsoft Office Pro Plus så att de överensstämmer med regleringen i GDPR.[247] Genom tilläggsavtalet har bl.a. reglerats i vilka specifika situationer Microsoft får hämta in telemetridata och hur data ska avidentifieras. Det innebär också ett förbud för Microsoft att använda kunddata för t.ex. profilering och reklam och en möjlighet för kunden att stänga av möjligheten till datainsamling. Avtalet innehåller dessutom bestämmelser om möjlighet för kunden att påkalla revision hos en utomstående part för att säkerställa att Microsoft hanterar data i enlighet med avtalet. Nederländernas regering har som ambition att göra tilläggsavtalet tillgängligt för hela offentliga sektorn inom EU.[248]

---

[244] Till exempel om en användare trycker backsteg flera gånger i rad och IP-nummer.

[245] Till exempel hämtas meddelandetitel.

[246] Ministry of Justice and Security Strategic Vendor Management Microsoft, *DPIA Office 365 ProPlus version 1905 (June 2019) Data protection impact assessment on the processing of diagnostic data* s. 76 ff

[247] Avtalet förhandlades fram av en myndighet under regeringen, Microsoft Strategic Vendor Management Office (SLM Rijk). Avtalet avser Microsoft Office Pro Plus förutom de mobila applikationerna och omfattar inte Microsoft Office 365.

[248] Se Strategic Vendor Management Microsoft for the Dutch Government and Ministerie van Veiligheid en Justitie *EU Software and Cloud Supplier Customer Council,* och Ministerie van Justitie en Veiligheid *Verificatie op de uitvoering van het overeengekomen verbeterplan met Microsoft (Ons kenmerk 2635551)* 2019-07-01.

Försäkringskassans allt ökande beroende av säkra, användarvänliga och robusta digitala tjänster innebär att myndigheten för egen del behöver klargöra om och när det är lämpligt och möjligt att använda de publika molntjänster som erbjuds av privata leverantörer.

Analysen i denna vitbok utgår från Försäkringskassans verksamhet. Det är dock vår förhoppning att den kan vara ett stöd även för andra myndigheter som vill utarbeta en digital strategi för sin samhällsbärande verksamhet.