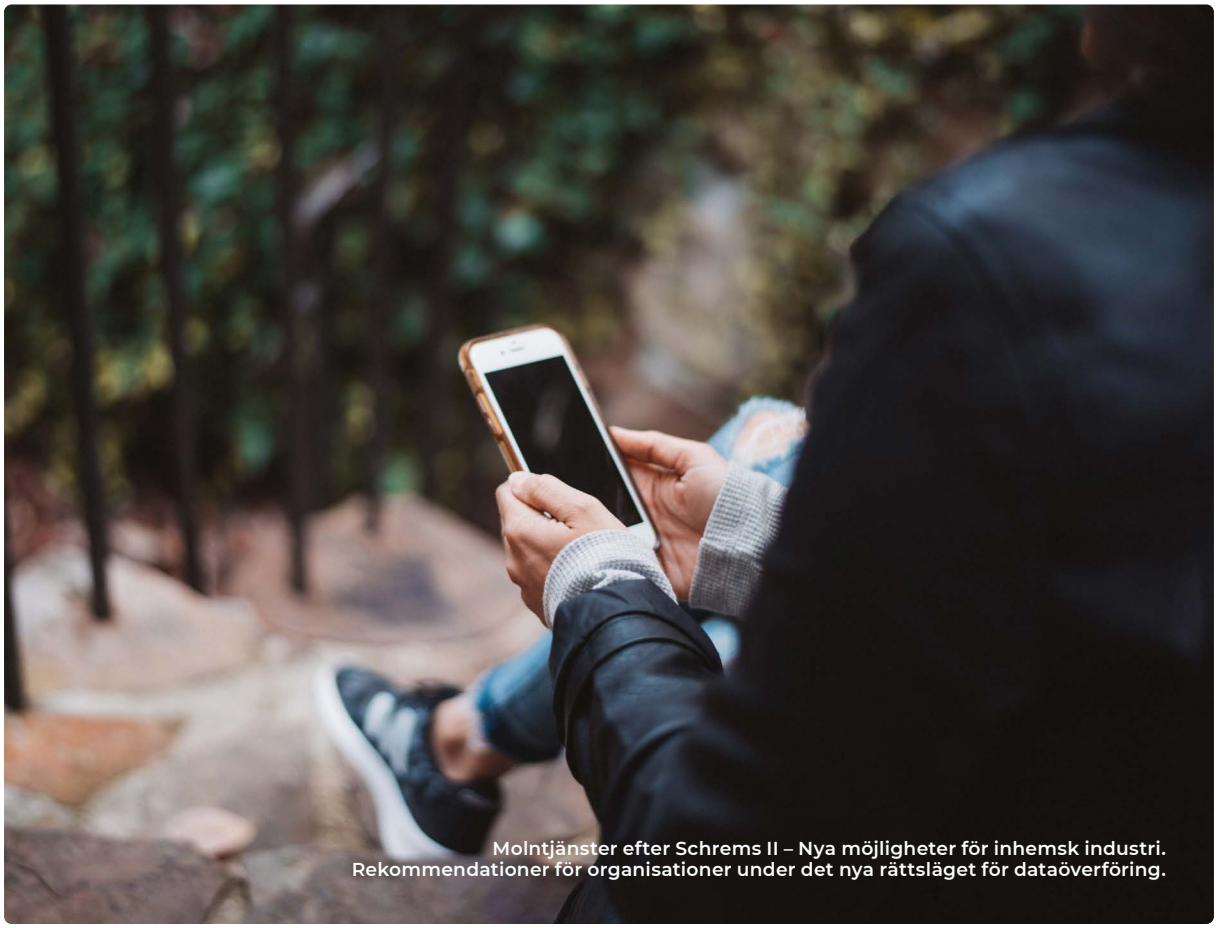
safespring

WHITE PAPER:

EU-domstolens ogiltigförklarande av Privacy Shield

Förutsättningar och rekommendationer för offentlig sektor och deras leverantörer

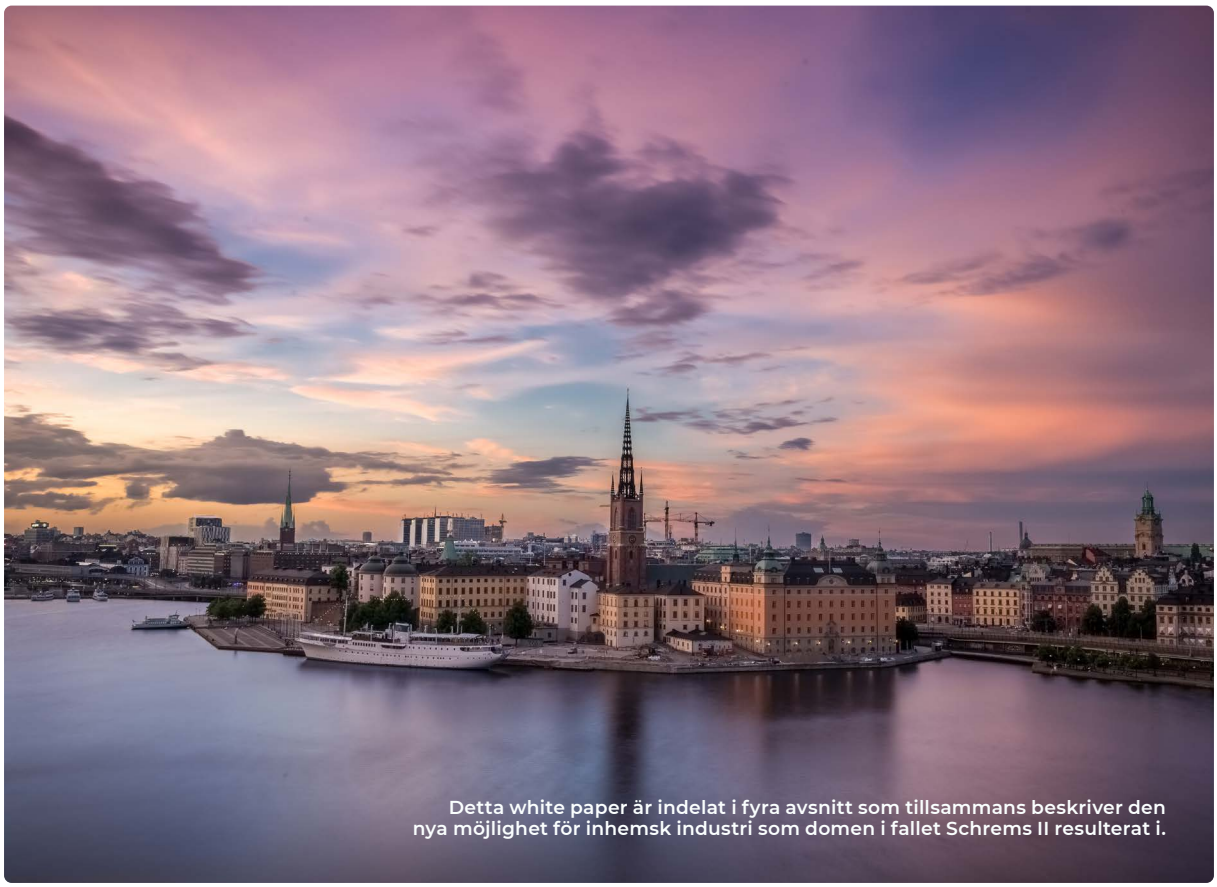


Bakgrund

Safespring publicerade under våren 2018 ett white paper om konsekvenserna av den europeiska dataskyddsförordningen (DSF) och amerikanska CLOUD Act på molnupphandlingar i Sverige.

Safesprings white paper avslutades med elva rekommendationer till organisationer som arbetar med molninfrastruktur i Sverige avseende dataskydd, datasäkerhet och jurisdiktionsfrågor. Nu har EU-domstolen i ett domslut 16 juli 2020 ytterligare preciserat villkoren för överföring av europeiska privatpersoners uppgifter till amerikansk jurisdiktion. Det påkallar en uppdatering av Safesprings tidigare rekommendationer. Det innevarande dokumentet går igenom Schrems II-avgörandet (del I), marknadsstrukturen för molntjänster och samverkan mellan tekniska krav och juridik (del II), olika svenska aktörers roll för vidareutvecklingen av denna marknadsstruktur och särskilt behovet av koordinering av insatser på statlig nivå (del III) och en kort beskrivning av vägen framåt (del IV). I del II och IV utvecklas Safesprings tidigare rekommendationer för organisationers egna verksamheter med anledning av det nya rättsläget. Del III ger organisationer bättre förutsättningar att ställa rätt krav på den statliga samordningen.

Innehåll



Detta white paper är indelat i fyra avsnitt som tillsammans beskriver den nya möjlighet för inhemsk industri som domen i fallet Schrems II resulterat i.

DEL I

Inledning – Ytterligare precisering av dataöverföringsregler i EU

Den 16 juli 2020 meddelade EU-domstolen sitt domslut i mål C-311/18, ofta benämnt ”Schrems II”.

Den 16 juli 2020 meddelade EU-domstolen sitt domslut i mål C-311/18[1] , ofta benämnt ”Schrems II”, rörande de europeiska konstitutionella principernas förenlighet med vad som fram till avgörandet föll var politiskt accepterade normer för dataöverföringar till tredjelandet USA. Huvudsakligen bekräftade domslutet vad EU-domstolen redan i ett antal avgöranden sedan Lissabonfördraget trädde i kraft 2009 gjort tydligt: dataskydd är en konstitutionell princip i EU-området (Art 8 i den europeiska stadgan för de grundläggande rättigheterna), och preciseringen av regler för upprätthållande av denna konstitutionella princip i exempelvis dataskyddsförordningen (DSF) undergräver inte denna konstitutionella princip.

I Schrems II konkretiseras att dessa konstitutionella normer medför att vissa delar av amerikansk underättelse- och säkerhetslagstiftning förhindrar företag som träffas av förpliktelser under denna lagstiftning från att anses vara säkra mottagare av data i europeisk juridisk bemärkelse. EU-domstolen påminner också europeiska politiker om att de administrativa dataöverföringsbeslut EU-kommissionen kan fatta enligt DSF Art 45 och överföringsavtal enligt DSF Art 46 och 49 inte kan användas för att åsidosätta de europeiska konstitutionella principerna om dataskydd.

Domslutet har konsekvenser för företag och myndigheter som behandlar europeiska medborgares personuppgifter i den meningen att utrymmet för avtal och samarbete med sådana aktörer som riskerar att träffas av förpliktelser under amerikansk lagstiftning avseende datautlämning till myndigheter nu är kraftigt begränsat.

Vad är ett dataöverföringsbeslut?

Dataöverföringsbeslut, eller beslut om adekvat skyddsnivå, innebär att EU-kommissionen beslutar att ett tredjeland har sådana normer som skyddar europeiska medborgares rättigheter. Ett dataöverföringsbeslut är inte ett avtal i egentlig mening, utan ett unilateralt förkunnande från EU-kommissionens sida.

EU-kommissionen fattar dock i praktiken inte beslut på egen hand, utan får stöd från den kommittée av medlemslandsrepresentanter som etablerats i DSF Art 93. EU-kommissionens beslut föregås ofta av förhandlingar med tredjelandet.

Vad är ett överföringsavtal?

Dataöverföringsavtal kan ta formen av standardiserade dataskyddsbestämmelser (DSF Art 46.2), biträdesavtal (DSF Art 46.3) eller avtal mellan näringsidkare och enskild (DSF Art 49).

Standardiserade dataskyddsbestämmelser ska innebära ett väsentligen likvärdigt skydd som den inhemska europeiska lagstiftningen.

EU-DOMSTOLEN HAR SÄRSKILT BESLUTAT

- Att tredjelands lagstiftning om säkerhet inte påverkar tillämpningen av europeiska rättigheter för medborgare, även om den europeiska medborgaren interagerar med näringsidkare från tredjelandet (C-311/18 para 89).
- Att kravet på ett väsentligen likvärdigt skydd för europeiska medborgares rättigheter vid dataöverföringar inte påverkas av den specifika mekanismen för överföringar som används (C-311/18 para 92).
- Att ”skyddsnivå” för personuppgifter ska vara väsentligen likvärdig med den som etableras inom EU-rätten, utan hänsyn till särskilda nationella bestämmelser i enskilda EU-länder (C-311/18 para 101 och 103).
- Att tredjeländers myndigheters möjligheter att bereda sig tillgång till uppgifter påverkar skyddsnivån (C-311/18 para 103).
- Att tillsynsmyndigheter har en skyldighet att agera då ett väsentligen likvärdigt skydd inte går att fastställa, särskilt då det saknas ett dataöverföringsbeslut (C-311/18 para 120-121).
- Att ett beslut från EU-kommissionen om standardavtalsklausuler inte påverkar skyldigheter för personuppgiftsansvariga och personuppgiftsmottagare att avbryta överföringar om det visar sig att skyddet som klausulerna omfattas inte kan realiseras (C-311/18 para 142).
- Att EU-kommissionens dataöverföringsbeslut ”Privacy Shield” är ogiltigt (C-311/18 para 201).

Huvudsakligen har EU-domstolen bekräftat de slutsatser som redan framkom i Safesprings white paper ”Hur du hanterar det osäkra läget i och med CLOUD Act och GDPR” från 2018. Medan den ekonomiska stressen av ytterligare spänningar mellan USA och EU i dataskyddsfrågor inte har underlättats vare sig av de politiska reaktionerna på Schrems I eller det nu meddelade Schrems II-beslutet, är den rättsliga situationen nu klarare.

I och med Schrems II-beslutet har det blivit tydligare att det inte framför allt är ett problem var datat som sådant lagras, utan var den aktör

Vad är leverantörslokalisering?

Schrems II-avgörandet förtydligar att det är leverantörslokalisering snarare än datalokalisering som begränsar möjligheterna för dataöverföringar till särskilt den amerikanska jurisdiktionen.

Skyddet för europeiska privatpersoner anses undergrävas då tredjelands myndigheter kan ålägga tredjelands tjänsteleverantörer förpliktelser som innebär att europeiska privatpersoner inte får det väsentligen likvärdiga skydd för sina uppgifter som de skulle ha åtnjutit inom unionens gränser.

Dessa slutsatser är inte nya i den europeiska rätten. Redan SOU 2017:74 om datalagring i brottsbekämpande syfte konstaterade att uppgiftslagring enligt europeisk rättspraxis är behäftad med krav på lokalisering.

Vad är ett tredjeland?

Ett tredjeland innebär under europeisk rätt ett land som inte är medlem i Europeiska unionen.

Vissa tredjeländer, exempelvis de som deltar i EFTA-samarbetet, har privilegierad status i förhållande till andra tredjeländer eftersom de förbundit sig att följa EU:s lagstiftning.

Andra tredjeländer, så som USA, Japan eller Indien, har inte sådan privilegierad status. Dataöverföringar regleras i DSF i förhållande till tredjeländer (DSF 5 kap.).

är placerad som lagrar datat. De rättigheter som kodifieras i europeisk rätt skyddar fysiska personer, och de skyldigheter att upprätthålla dessa rättigheter som kodifieras i europeisk rätt träffar fysiska och juridiska personer. Om tredjelands lagstiftning är gällande gentemot en fysisk eller juridisk person på sådant sätt att denna förhindras från att upprätthålla skyldigheter avseende grundläggande rättigheter för en fysisk person, är detta alltså i princip ett betydelsefullt hinder för samverkan med denna fysiska eller juridiska person.

Domslutet återaktualiserar Safesprings rekommendationer till organisationer gällande molntjänster.[2] Men organisationer behöver inte bara se till att de har en grundlig juridisk analys av datakataloger och rättsliga grunder för personuppgiftsbehandlingar och -överföringar, utan bör även säkerställa att tjänster de begagnar sig av använder öppet specificerade protokoll och är tekniskt konstruerade med avsikten att möjliggöra eventuella framtida leverantörsbyten. Vid investeringar i eller användning av molntjänster som i något marknadsled kan komma att röra (europeiska) myndigheters behandling av personuppgifter förefaller samverkan med amerikanska företag vara i princip uteslutet, så länge USA inte förändrar sin inhemska lagstiftning till europeiska rättssubjekts fördel.

Detta sista villkor kommer vara särskilt intressant vid den av EU-kommissionen annonserade processen att inleda samtal om ett nytt dataöverföringsbeslut[3].

I och med Schrems II-beslutet har det blivit tydligare att det inte framför allt är ett problem var datat som sådant lagras, utan vilket lands jurisdiktion leverantören lyder under.

DEL II

Molnet – Lokal infrastruktur med lokal anpassning

Molntjänster har inneburit stora möjligheter för organisationer att effektivisera och automatisera sitt arbete.

Det är framför allt genom stordriftsfördelar som molntjänster bidrar till allt ifrån miljömässig hållbarhet till starkare säkerhetsarbete, men även ökad förmåga att snabbt få tillgång till antingen datalagringskapacitet eller databehandlingskapacitet utan formaliserade upphandlingar har bidragit till att denna moderna form av IT-drift gjort framsteg inte bara i privat sektor utan även i offentlig.[4]

Fördelarna med viss centralisering visar sig också i ökad anpassningsbarhet. Kostnader för utveckling och underhåll av grundfunktionaliteter kan spridas ut på flera olika parter. Ett flertal globala konsortier har upprättats de senaste 10 åren med uppdrag att underhålla och utveckla nyttiga basfunktioner vid hantering av stora antal servrar.[5] Sysslor som i ett mindre IT-system kan ta många manuella timmar i anspråk går i stordriftsmiljöer att automatisera, och normalt tidskrävande och dyra sysslor som investeringar i realtidsbevakning av IT-miljöns säkerhet eller åtgärder mot säkerhetsbrister blir lättare att motivera. Med säkra och optimerade grundfunktioner som bas kan sedan specialiserade tjänster byggas till och anpassas efter varje verksamhets särskilda behov. Verksamheten kan förlita sig på en stabil och gedigen grund, utan att den måste bygga upp en hel IT-arkitektur från grunden varje gång ett nytt koncept ska prövas.

Det stora intresset för molntjänster har gjort att marknaden snabbt utvecklats till att innefatta en rad olika tjänster med olika fördelar för upphandlande kund. Olika grader av automatisering och stordrift kan medges beroende på de specifika krav som gäller inom varje upphandlande organisation.

Således innefattar beteckningen molntjänst dels centraliserad hantering av infrastruktur – virtualiserade servrar med ett operativsystem som kunden själv kan disponera efter eget tycke, och genom att själv tillfoga och underhålla specifika tjänster för specifika ändamål (exempelvis databaser, webbservrar eller administrativa system). Dels innefattas ändamålsspecifika system där leverantören av molntjänsten själv bistår med databasverktyg och andra grundläggande byggstenar för mer specialiserad funktionalitet. Den mest synliga delen av molnmarknaden för en typisk slutkonsument utgörs av sådana tjänster som redan av molntjänstleverantören är högt förädlade: Centraliserade system för allt ifrån textredigering till schemaläggning och videokonferenser.

Molnmarknaden har därtill utvecklats så att olika sorters molntjänster samverkar med varandra i B2B-relationer. En förädlad molntjänst i form av ett personalliggarsystem kan alltså samverka med en mer infrastrukturell molntjänst som tillhandahåller virtuella servrar. På så sätt behöver en slutkund bara hantera själva inmatningen och verifikationen av relevanta uppgifter snarare än underhåll och administration av kodbaser och underliggande operativsystem. Det är också vanligt att både infrastrukturella tjänster och förädlade tjänster tillhandahålls från samma marknadsaktör. Precis som telekommarknaden på 1980-talet präglades av vertikal integration är också molnmarknaden idag dominerad av

aktörer med en hög nivå av vertikal integration. Med det menas att företagen samtidigt tillhandahåller både infrastruktur, plattformar och mjukvaror.

För upphandlande slutkonsumenter behöver för- och nackdelar med vertikal integration noggrannt övervägas. I en vertikalt separerad marknad där många olika företag kan bidra med nya funktionaliteter på varje nivå i värdekedjan finns större utrymme för varierat och anpassat tjänsteutbud. Dessutom hamnar stora slutkonsumenter i bättre kunskapsläge gentemot leverantörerna. Precis som vertikal separation och konkurrens på telekommarknaden öppnade för utveckling av nydanande tjänster på 1990-talet, kan separation och konkurrens på molnmarknaden skapa utrymme för nydanande tjänster på 2020-talet.

En viktig skillnad är att molnmarknaden redan i hög utsträckning utgår ifrån gränsöverskridande och gemensamma öppna kodbaser. Marknadens ursprung är globalt, inte nationellt, och en högre nivå av vertikal separation behöver inte innebära en högre grad av nationalisering. Det gör att både applikationer, beräkningskraft och data som matas in i dessa applikationer är

geografiskt och organisatoriskt rörliga. Dataöverföringar har blivit vanliga både i gränsöverskridande bemärkelse och i bemärkelsen att data överförs mellan organisationer som vardera fyller en egen roll i leveransen av den slutgiltiga tjänsten.

Ett tyskt projekt som försöker förena erfarenheter från telekomindustrin med nyttorna från molnindustrin är GAIA-X[6], ett ramverk för kostnadsdelning mellan geografiskt knutna aktörer som tillhandahåller interoperabla tjänster.[7] I Frankrike har man sedan snart ett årtionde understrukit att upphandlingsinstrument kan vara särskilt lämpliga för att stärka europeiska småföretags roll i digitala ekosystem, med särskild tonvikt vid just lösningar för öppna data och molntjänster.[8]

Med flexibilitet följer ökat ansvar

Användning av molntjänster innebär i praktiken att data som en upphandlande organisation ansvarar för, och applikationer som använder sådan data som input, kommer att befinna sig på infrastruktur som inte administreras av organisationen själv. Oavsett vilken nivå av förädling organisationer väljer för sina molntjänster är många av stordriftsfördelarna avhängiga att den faktiska administratören av molntjänstens infrastruktur har tillgång till tillräcklig information om den data som behandlas för att kunna tillgängliggöra de resurser och säkerställa den säkerhetsnivå som kunden kräver. Det är i denna tekniska oundviklighet som skyldigheter för upphandlande organisationer uppstår i förhållande till EU-domstolens Schrems II-avgöranden.

EU-domstolens bedömning av grundläggande rättigheter i EU-området skapar ett krav på personuppgiftsansvariga organisationer att skaffa sig en överblick över hela värdekedjan, även då man upphandlar en specifik och avgränsad mjukvaruapplikation som bara ska åstadkomma en avgränsad nytta i den egna verksamheten. Slutkonsumenten bör inte bara överväga fördelarna med den tjänst man upphandlar, utan också titta på hur denna tjänsteleverantör interagerar med underleverantörer.

Redan i den statliga utredningen ”Den osynliga infrastrukturen” från 2007 observerades[9] att ”[IT]-infrastruktur har den egenheten att den är osynlig i de fall standarder finns på plats och är ändamålsenliga. Först när [standarder] saknas märks deras frånvaro och skapar problem. IT-standarder är också i stor utsträckning osynliga i beslutsfattandet hos verksamhetsansvariga. Verksamhetsbeslut, till exempel om upphandling av e-tjänster, innebär ofta beslut också om val av standarder, men dessa tycks inte beslutas separat och uttryckligen, åtminstone på den verksamhetsansvariga nivån, utan blir en outtalad konsekvens av verksamhetsbeslut av olika slag.” En av följderna av både DSF och Schrems II-beslutet bör vara att dessa outtalade konsekvenser i själva verket måste uttalas.

Personuppgiftsbiträden ska säkerställa att eventuella underbiträden lyder under samma avtalsrättsliga förpliktelser gentemot enskilda vars uppgifter behandlas av en personuppgiftsansvarig som personuppgiftsbiträdet själv (DSF Art. 28).

Det är dock upp till personuppgiftsansvarig att i slutändan säkerställa att både biträden och underleverantörer har möjlighet att uppfylla rätt sorts avtalsrättsliga garantier. När antingen ett biträde eller biträdets underleverantör träffas av rättsliga förpliktelser i ett tredjeland, menar EU-domstolen att den personuppgiftsansvarige har ett omfattande ansvar att säkerställa att dessa rättsliga förpliktelser inte försämrar europeiska medborgares dataskydd. EU-domstolen menar därtill att den personuppgiftsansvariges skyldigheter inte minskas bara för att det inte går att konstatera en faktisk realisering av sådana rättsliga förpliktelser på specifika uppgifter, utan att det räcker med att en sådan rättslig förpliktelse kan uppstå (jfr C-311/18 para 142).

Safesprings checklista från 2018 tar upp de

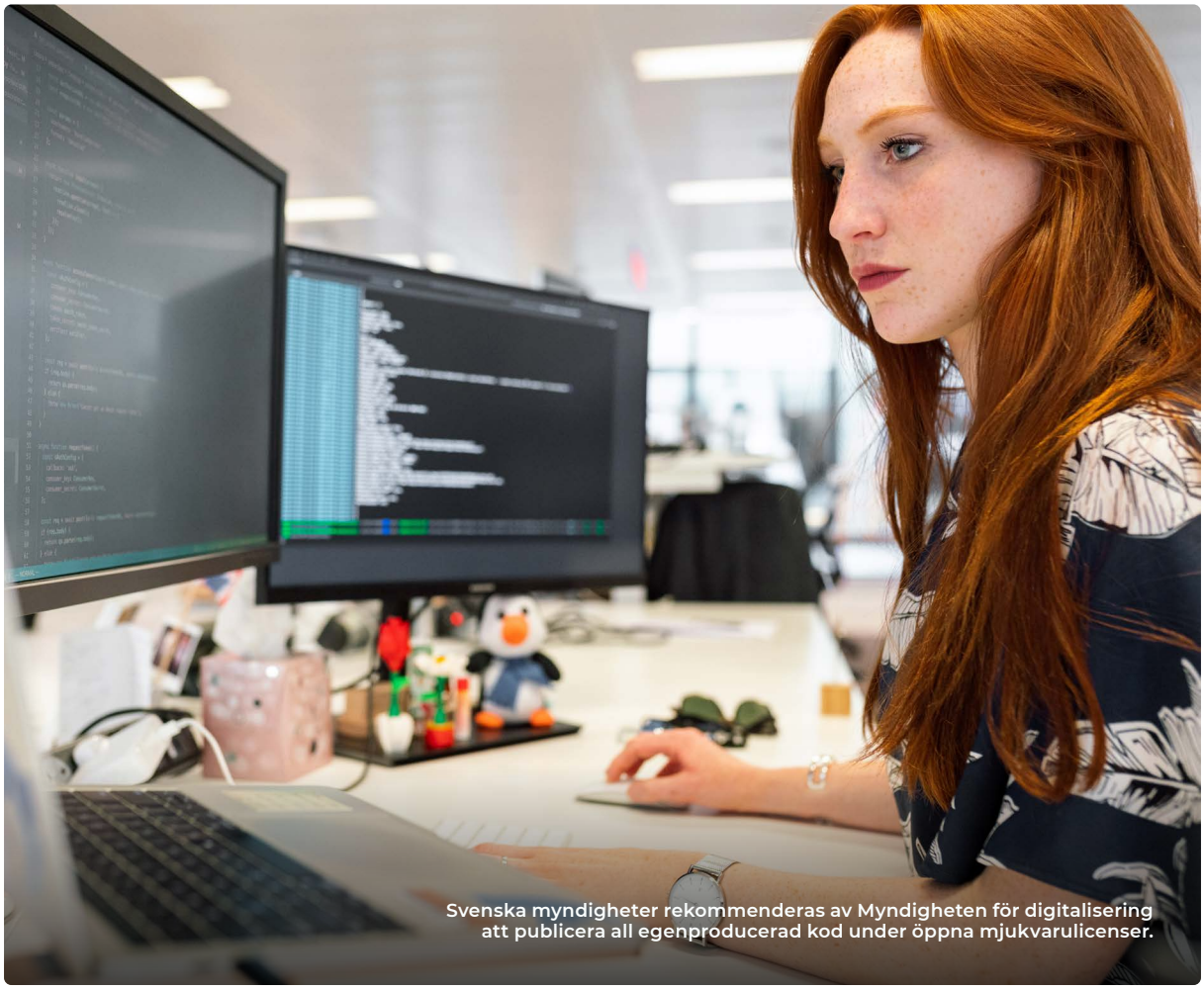
Gör en grundlig kontroll av tjänsteleverantören och dess underleverantörer.

frågeställningar som varje organisation bör tillämpa vid valet av infrastruktur.[10] I ljuset av Schrems II-avgörandet behövs det i denna checklista förtydligas så att molntjänstleverantörer som sorterar under tredjelands lagstiftning bör ha svårt att uppfylla EU-rättens krav. För särskilt tredjelandet USA gäller att den amerikanska lagstiftningen behöver förändras för att företag baserade i landet ska vara en ur dataskyddsrättsligt hänseende godtagbar mottagare av uppgifter. Det räcker inte längre att hålla reda på vilka (känsliga) personuppgifter som kan komma att hamna hos en utländsk myndighet, utan risken för att sådana uppgifter kan krävas utlämnade behöver nu aktivt förbyggas.

Det innebär i praktiken att upphandlande organisationer bör begränsa sina val av tjänsteleverantörer och underleverantörer till sådana leverantörer som är juridiskt baserade någonstans inom EEA-området. Det kan också finnas behov av att säkerställa att administration och underhåll av IT-system inte utförs av personer som är verksamma utanför EEA-området. Att europeiska politiker och EU-kommissionen två gånger misslyckats med att formulera dataöverföringsbeslut med tillräckligt starka garantier för dataskydd bör också få upphandlande organisationer att tveka inför att förlita sig på framtida dataöverföringsbeslut.[11] I praktiken har svenska politiker trots begränsat rättsligt utrymme att kringgå EU-domstolen ändå huvudsakligen orienterat insatser mot försök att bevara status quo,[12] med följd att de aktörer som följer politiska riktlinjer riskerar att hamna rättsligt fel.

KOMPLETTERANDE REKOMMENDATIONER [13]

1. Kontrollera ifall tjänsteleverantörer i rakt nedstigande led använder underleverantörer i form av PaaS eller SaaS-tillhandahållare.
2. Kontrollera ifall tjänsteleverantören vid utformingen av sin tjänst använt öppet specificerade mjukvarufunktionaliteter (som API:er eller dataformat).
3. Verifiera att det finns avtal mellan tjänsteleverantören och underleverantören, samt att avtalet överensstämmer med de dataskyddsrättsliga kraven.
4. Kontrollera att underleverantören tillhandahåller dokumentation kring de öppna standarder och specifikationer underleverantören använt för sina infrastrukturlösningar. Kontrollera vidare att tjänsteleverantören förvissat sig om att de har möjlighet att vid behov migrera till en annan underleverantör.
5. Kontrollera ifall antingen tjänsteleverantören som sådan eller tjänsteleverantörens underleverantörer har sin legala hemvist i tredjeland. Gör en bedömning av om detta riskerar innebära att tredjelandets myndigheter kan ålägga antingen underleverantören eller tjänsteleverantören att överlämna uppgifter till tredjelandets myndigheter.



Svenska myndigheter rekommenderas av Myndigheten för digitalisering att publicera all egenproducerad kod under öppna mjukvarulicenser.

Öppenhet ett skydd mot politisk instabilitet

På både europeisk[14] och svensk[15] nivå har det understrukits att starkare fokus på öppet tillgänglig programkod och öppna standarder skapar både insyn och överskådlighet på det sätt som den europeiska dataskyddsrätten nu förefaller kräva. Svenska myndigheter rekommenderas av Myndigheten för digitalisering att publicera all egenproducerad kod under öppna mjukvarulicenser.[16]

Öppna standarder och öppna kodbaser är inte rekommendationer som härrör från den europeiska dataskyddsrätten. Däremot skapar de större rörlighet för slutkonsumenter mellan olika leverantörer. Om infrastrukturen är öppen och interoperabel har slutkonsumenten större frihet att anpassa sig efter exempelvis domstolsavgöranden.

Även om dataskyddsrätten inte som sådan påbjuder att organisationer ska säkerställa en möjlighet att byta leverantör, förefaller praxisutvecklingen inom dataskyddsrätten vara sådan att organisationer möjligen kan vilja investera i sådan flexibilitet själva.

I fråga om dataöverföringar har exempelvis det politiska ledarskapet i Sverige och Europa inte bara en, utan två gånger felkalibrerat politiska beslut på sådant sätt att EU-domstolen tvingats riva upp dem. För organisationer som behöver följa gällande rätt innebär detta höga kostnader och stor osäkerhet och tidsåtgång. Medvetna satsningar på öppna standarder och kod minskar dock friktionen vid förändringsbehov.

DEL III

Rättsliga regelverk är ett gemensamt ansvar

Varje enskild organisation bör dock inte tvingas att på egen hand uppfinna sätt att hantera öppna standader och dataskyddsrätt.

I fråga om dataöverföringar och molntjänster finns ett antal svenska statliga aktörer vars insatser kan göra det enklare för andra att anpassa sig till EU-rätten, samtidigt som en hög nivå av både grundstabilitet och applikationsstabilitet uppnås i IT-systemen.

För svenska organisationer görs här bedömningen att följande aktörer bör uppmuntras att arbeta vidare med IT-infrastrukturer och dataskydd:

1. **UTREDNINGEN** som etablerades genom kommittéedirektiv 2019:64, med tilläggsdirektiv i 2020:73, bör inte enbart ges mer tid att slutföra sitt uppdrag utan även få substantiellt tydligare mandat att titta på dataöverföringsfrågor och öppna standarder.
    - Uppdragsställaren bör efterfråga en uppföljning av de slutsatser i SOU 2017:74 som innebar att data som lagras av telekomoperatörer ska lagras inom Sverige i förhållande till data som lagras av andra aktörer.
    - Uppdragsställaren bör även efterfråga en uppföljning av målsättningarna i SOU 2007:47 kap. 6 utifrån de senaste 15 årens europeiska och svenska rättsutveckling, med avseende på de institutionella förutsättningar för interoperabel, laglig och fungerande teknisk infrastuktur som föreslås där.
    - Uppdragsställaren bör efterfråga en sammanställning av hur andra EU-länder arbetar med dataöverföringar och molninfrastrukturer. Exempelvis har Slovenien påbörjat arbetet med ett regeringsmoln[17], och Frankrike anammat en uttalad strategi för ”digital suveränitet”.[18] De här åtgärderna bör kontrasteras och jämföras med innevarande svenska strategier för IT-infrastruktur och molntjänster.
    - Huvudsakligen bör uppdragsställaren förtydliga att utredaren inte bara ska titta på hur redan befintliga avtal mellan kommuner och företag i tredjeland kan göras lagliga, utan ge utredaren mandat att föreslå vägar framåt som räcker även över nästa dataskyddsprövning i EU-domstolen.

Det statliga IT-arbetet behöver struktur, målmedvetenhet, samordning. Foto: Matthew Broadley

2. **DET SVENSKA JUSTITIEDEPARTEMENTET** har möjligheter att följa EU-kommissionens förhandlingar med den amerikanska administrationen om ett nytt dataöverföringsbeslut genom den så kallade Artikel 93-kommittéen (som etableras av DSF Art. 93). Inför förhandlingarna om Privacy Shield uppgav Justitiedepartementet att de framför allt haft skriftlig kontakt med det svenska företaget Ericsson,[19] och Sveriges regering drev också på för ett snabbt beslut som inte ställde ultimata krav på USA.[20] Schrems II-beslutet visar att detta förhållningssätt lider av vissa tillkortakommanden, och en större bredd på input till justitiedepartementet skulle kunna vägleda regeringen att söka stabilare lösningar på dataöverföringsfrågorna.

3. **DATAINSPEKTIONEN** bör ges ett skarpare uppdrag att arbeta vidare med tillsyn och föreskrifter. I en utredning från Statskontoret[21] påtalades sommaren 2020 att myndigheten lider av en ”försiktighetskultur”, som i just fallet med molntjänster och dataöverföringar riskerar att förvärra och förlänga den rättsliga osäkerheten. I SOU 2016:65 framgår att Datainspektionen ibland även haft problem att samverka med andra myndigheter. Ett explicit mandat att bedriva tillsyn och samverka med andra myndigheter kring särskilda problemområden (så som upphandling, IT-infrastruktur och dataöverföringar), skulle kunna ge större tydlighet åt fler aktörer på svenska marknaden.

4. **KONKURRENSVERKET** bör ges ett uppdrag att följa upp den genomlysning av ansvarsfördelningen mellan personuppgiftsbiträden och personuppgiftsansvariga som Datainspektionen annonserade för i sin tillsynsplan 2019-2020.[22] Särskilt bör Konkurrensverket utifrån sitt tillsynsuppdrag under lagen om offentlig upphandling titta på hur Datainspektionens slutsatser påverkar möjligheter och utmaningar för upphandlare i offentlig sektor, i förhållande till de ramavtal[23] som redan finns tillgängliga från Statens inköpscentral (Kammarkollegiet), möjligen i samverkan med Datainspektionen.

5. **TILLVÄXTVERKET** bör ges i uppdrag att utreda svenska möjligheter inom ramen för det tyska projektet GAIA-X.[24] Möjliga riktningar på detta arbete kan vara att utreda huruvida affärsmodellerna som föreslås av GAIA-X är tillräckligt framtidsanpassade, eller i vilken utsträckning GAIA-X kan innebära fördelar för svenska moln- och IT-aktörer som inte kan uppnås inom ramen för de privata konsortier som utvecklar öppna molninfrastukturer (ex. OSF[25]) eller orkestreringsverktyg (ex. CNCF[26]). Därtill vore en genomlysning av svenska aktörers nyttor från det europeiska ISA2-projektet[27] välkommen, också utifrån potentiella framtidsmöjligheter för svensk industri.

Det statliga IT-arbetet behöver struktur och målmedvetenhet, och olika myndigheters uppdrag och styrkor behöver samordnas för ett enhetligt utfall. Ramarna för möjliga utfall är i viss utsträckning redan förutbestämda av den EU-rättsliga koordinering som Sverige underställt sig i och med medlemskapet i Unionen. Regeringens möjligheter att bistå svenska organisationer med adekvat stöd i dessa frågor är också i hög utsträckning avhängig samma organisationers förmåga att tydligt kommunicera sina problem till relevanta makthavare på nationell nivå. Schems II-beslutet bör ses som en möjlighet att snabbare uppnå en hög grad av klarhet, i stället för som ett hinder.

Organisationer bör utarbeta en plan för att migrera bort från molntjänster som sorterar under amerikansk lagstiftning.

DEL IV

Vägar framåt

Organisationer i Sverige är i dagsläget sannolikt förhindrade från att välja molntjänster som lyder under amerikansk lagtiftning vid upphandlingar.

Anledningen till detta återfinns i amerikansk lagstiftning kring underrättelseverksamhet, men också den CLOUD Act som Safespring redan i tidigare white papers har berörts. Mot bakgrund av detta bör organisationer, utöver att följa Safesprings redan befintliga rekommendationer och de förstärkningar som nämnts ovan

- **UTARBETA EN PLAN** för att migrera bort från molntjänster som sorterar under amerikansk lagstiftning.[28]
- **SE ÖVER** hur den egna organisationen redan arbetar med befintliga riktlinjer från Statens inköpscentral, eSam och ISA2 (exempelvis genom att utvärdera befintliga projekt utifrån redan existerande rekommendationer).
- **AKTIVT ENGAGERA** regeringen i utveckling av en svensk plan för molntjänster som är förenliga med europeisk rätt.

Källhänvisning

Detta white paper är skrivet av Amelia Andersdotter. Safespring erbjuder svenskproducerade molntjänster.

1. ECLI:EU:C:2020:559
2. Safespring, White paper: Hur du hanterar det osäkra läget i och med CLOUD Act och GDPR, 2018
3. EU-kommissionen, 10 augusti 2020, Joint Press Statement from European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Wilbur Ross. https://ec.europa.eu/info/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-ross-7-august-2020-2020-aug-07_en
4. Statens servicecenter, En gemensam statlig molntjänst för myndigheternas it-drift, delrapport 2017.
5. Jfr OpenStack Foundation (OSF) och Cloud Native Computing Foundation (CNCF).
6. GAIA-X: a federated data infrastructure for Europe. https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html
7. Interoperabilitet: samverkan mellan olika komponenter. Se också SOU 2007:47, s. 133 ff.
8. Rapport d'Information No 443, Union européenne -- colonie du monde numérique ?, 20 mars 2013, s. 115-116.
9. SOU 2007:47, Den osynliga infrastrukturen, s. 64.
10. Jfr ovan fotnot 2.
11. Både Safe Harbor-beslutet från 2001 och Privacy Shield-beslutet från 2016 har funnits ogiltiga av EU-domstolen.
12. Jfr kommittéedirektiv 2019:64 med tillägg i dir. 2020:73.
13. Se Rekommendationer för organisation i ovan, fotnot 2.
14. C(2018) 7118, European Commission Digital Strategy - A digitally transformed, user-focused and data-driven Commission, 2018.
15. E-delegationen, Vägledning för digital samverkan, Version 4.1, 2015-05-28.
16. DIGG, 2019-136, Policy för utveckling av programvara.
17. Slovenian State Cloud DRO, https://nio.gov.si/nio/asset/drzavni+racunalniski+oblak+dro?lang=en
18. Se ovan, fotnot 8.
19. Enligt grundlagsenhetens diarium, efterfrågat hösten 2016 av författaren.
20. Justitiedepartementets instruktion inför sammanträde i kommittén för skydd av enskilda med avseende på behandling av personuppgifter av 2016–06–20.
21. Statskontoret 2020:14, Myndighetsanalys av Datainspektionen.
22. Datainspektionen DI-2019-841, 15 mars 2019.
23. Kammarkollegiet, Statens inköpscentral, ramavtal på IT- och telekomområdet. https://www.avropa.se/ramavtal/ramavtalsomraden/it-och-telekom/
24. Se ovan fotnot 6.
25. Open Stack Foundation https://osf.dev
26. Cloud Native Computing Foundation (Linux Foundation) https://cncf.io
27. Europakommissionen, Interoperability solutions for public administrations, businesses and citizens. https://ec.europa.eu/isa2/
28. Fråga 5 i del II kommer i princip alltid att behöva besvaras jakande vid användning av amerikanska molntjänster, så länge USA inte ändrar sin lagstiftning.

Safespring är din säkra källa för infrastrukturtjänster

Besök gärna vår webbplats för att lära dig med om molntjänster och hur Safespring kan lösa dina behov av Backup, Storage och Compute.

www.safespring.se

safespring

+46 (0)8-55 10 73 70 | info@safespring.com
Smidesvägen 12, 171 41 Solna, Sweden

www.safespring.se