Polisen

Polismyndigheten

Datum
2021-04-30

Diarienr (åberopas) A065.323/2021
Saknr 000
Er referens I2021/00342

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

It-driftsutredningens delbetänkande Säker och kostnadseffektiv it-drift - rättsliga förutsättningar för utkontraktering, SOU 2021:1

Sammanfattning

Polismyndigheten avstyrker att utredningens förslag genomförs då det inte synes underlätta eller tydliggöra för myndigheter, kommuner eller regioner när, om och hur de kan utkontraktera it-drift avseende teknisk bearbetning och teknisk lagring av uppgifter. Vidare efterlyser Polismyndigheten en analys om och hur direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation kan påverka utredningens tolkningar och förslag.

Polismyndigheten delar inte de bedömningar utredningen gjort avseende begreppen *röjande* och *tredjelandsöverföring*. Detta mot bakgrund av att innebörderna av begreppen är ifrågasatta och oklara samt att de tolkningar som slås fast i utredningen synes gå utöver befintlig praxis från EU-domstolen. Polismyndigheten anser härutöver att det behöver tydliggöras hur innebörderna av begreppen förhåller sig till varandra. Polismyndigheten saknar en analys av vilka konsekvenser som bedömningarna generellt kan få i svensk rätt och i förhållande till att svensk rätt måste vara förenlig med EU-rätten.

Om utredningens förslag ändå genomförs anser Polismyndigheten att det krävs att en tydlig vägledning för hur intresseavvägningen mellan utkontraktering och sekretess tas fram, vilken måste överensstämma med gällande EU-rätt. Vidare att det görs en sammantagen, genomgripande och entydig analys av innebörden av begreppen *röjd* och *tredjelandsöverföring* som också innefattar en utförlig konsekvensanalys.

Polismyndighetens synpunkter

Synpunkterna nedan följer den struktur och numrering som framgår av utredningen.

6. Säkerhetsskydd och informationssäkerhet

6.2.12 Särskilt om aggregerad och ackumulerad information

Polismyndigheten gör bedömningen att det är olämpligt att det vid utkontraktering av teknisk bearbetning och teknisk lagring är tjänsteleverantören som ska ta ställning till det samlade skyddsvärdet av alla uppgifter som flera verksamhetsutövare lämnar ut till leverantören för Sveriges säkerhet. Det är i princip omöjligt för en stor internationell tjänsteleverantör att göra en samlad bedömning om leverantören anlitas av många verksamhetsutövare vilket skapar säkerhetsrisker.

7. Dataskydd

7.2 Dataskyddsregleringen

Polismyndigheten saknar en samlad, övergripande och entydig analys i betänkandet gällande innebörden av begreppen *röjande* och *överföring till tredjeland* satt i relation med varandra (se vidare avsnitt 9.8 nedan). Detta också med beaktande av de regulatoriska skillnaderna mellan hanteringen av offentliga och sekretessbelagda personuppgifter samt offentliga och sekretessbelagda uppgifter som inte utgör personuppgifter. Personuppgifter regleras genom dataskyddsregelverket vilket till största del styrs av EU-rätten medan offentlighet och sekretess generellt styrs av svensk reglering utan inblandning av EU-rätten.

7.4 Tredjelandsöverföring enligt dataskyddsförordningen

Polismyndighetens bedömning är att den tolkning som slås fast i utredningen gällande tredjelandsöverföringar är självmotsägande och det finns risk att den kan komma att strida mot EU-rätten. Den tolkning som görs av utredningen är i dagsläget inte fastslagen av EU-domstolen.

7.4.3 Vad avses med en tredjelandsöverföring av personuppgifter?

Polismyndigheten ser inte att den tolkning som utredningen gör av vad som utgör tredjelandsöverföring går att utläsa i befintlig rättspraxis från EU-domstolen.

Utredningen slår å ena sidan fast att det utgör en överföring av personuppgifter till tredjeland när en tjänsteleverantör behandlar personuppgifter genom användning av utrustning som finns i tredjeland, oavsett hur lång eller kort tid som utrustningen används och om uppgifterna är krypterade eller pseudonymiserade. Å andra sidan slår utredningen fast att tredjelandsöverföring inte sker när uppgifter överförs till ett företag som lyder under extraterritoriell lagstiftning utanför EU/EES men som är etablerat i EU (se även avsnitt 9.8.3 nedan). En överföring anses enligt utredningen ske först i samband med att uppgifterna överförs till myndigheter eller annan mottagare i ett tredjeland.

En överföring av personuppgifter till tredjeland är enligt Integritetsskyddsmyndigheten (IMY) ”… när personuppgifter blir *tillgängliga* för någon i ett

land utanför EU/EES-området [kursivering införd]."[1] Den europeiska dataskyddsombudsmannen (EDPS) har gett uttryck för motsvarande uppfattning.[2] Det kan även nämnas Säkerhetspolisens föreskrifter om säkerhetsskydd, PMFS 2019:2, där det framgår att det är *tillgång*, och inte överföring, av uppgifter som regleras.[3]

Den sekretessbrytande regeln som föreslås av utredningen synes enligt Polismyndigheten innebära att, efter en intresseavvägning samt beaktande av personuppgiftsansvariges omsorgsplikt, utredningen ser det som oproblematiskt att lämna ut personuppgifter till tjänsteleverantörer som lyder under exempelvis US CLOUD Act. Polismyndigheten menar att denna tolkning inte är fastslagen av EU-domstolen och riskerar att strida mot EU-rätten, som har företräde framför svensk rätt. Uppgifter som utgör personuppgifter kommer härutöver att hanteras annorlunda i förhållande till icke-personuppgifter då de senare i princip inte omfattas av det EU-rättsliga regelverket utan enbart av den svenska regleringen avseende offentlighet och sekretess.

7.4.8 Rättsläget avseende överföringar av personuppgifter till USA[4]

Polismyndigheten ställer sig tveksam till att utredningen utifrån uttalanden i Schrems II-domen[5] synes göra bedömning att en överföring till USA aldrig kan vara tillåten. Det vill säga, att det inte är tillåtet att överföra uppgifter ens i enskilda fall vid tillämpningen av någon undantagssituation i artikel 49 i dataskyddsförordningen, och att denna bedömning omfattar även situationer där det inte är fråga om utkontraktering. Utredningen synes ha svårt att se att det finns några ytterligare skyddsåtgärder som kan vidtas som läker de brister som EU-domstolen bedömer finns i amerikansk lagstiftning. Det råder olika uppfattningar i frågan om domens innebörd och utredningens bedömning tycks inte stå helt i överensstämmelse med exempelvis IMY:s syn, som i sin tur hänvisar till Europeiska dataskyddsstyrelsen (EDPB).[6]

Vidare ställer sig Polismyndigheten tveksam till att likna dataskyddsförordningen och brottsdatalagens bestämmelser om överföring till tredjeland alltför mycket, samt till att dra generella slutsatser som utredningen tycks göra.[7]

---

[1] https://www.imy.se/lagar--regler/dataskyddsforordningen/tredjelandsoverforing/, "Överföring av personuppgifter till tredje land är när personuppgifter blir tillgängliga för någon i ett land utanför EU/EES-området."

[2] Se European Data Protection Supervisor (EDPS), *The transfer of personal data to third countries and international organisations by EU institutions and bodies*, position paper, 14 juni 2014, s. 6 f. Se även Europeiska dataskyddsstyrelsen, *Rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelsen med EU-nivån för skydd av personuppgifter*, 10 november 2020, not 22, där det framhålls att "… fjärråtkomst av en enhet i ett tredjeland till uppgifter som finns inom EES också betraktas som en överföring."

[3] Se exempelvis PMFS 2018:2, 7 kap 3§.

[4] Synpunkterna avseende detta avsnitt har koppling även till avsnitten 7.4.5, 7.4.6, 7.5 och 7.6.

[5] Mål C-311/18, *Data Protection Commissioner* mot *Facebook Ireland Limited och Maximillian Schrems*, (*Schrems II*), ECLI:EU:C:2020:559.

[6] se t.ex. Integritetsskyddsmyndighetens hemsida, Frågor och svar om Schrems II-domen.

[7] Jfr avsnitt 7.5 och 7.6, sammanfattande avsnitt, i utredningen.

8. Offentlighet, sekretess och tystnadsplikt

8.9 Röjandebegreppet

Polismyndigheten menar att den tolkning som utredningen gör av röjandebegreppet, där alla uppgifter som lämnas ut ska anses såsom röjd, riskerar att skapa otydligheter och inkonsekvenser i svensk rätt. Polismyndigheten anser därför att en mer genomgripande analys av den rättsliga innebörden av begreppen *röja*, *lämna ut* och *överföring* och hur dessa relaterar till varandra i ljuset av det underliggande syftet med sekretess och dataskydd behövs.

Uppgifter ska enligt utredningen anses såsom röjda i OSL:s mening så snart de lämnas ut vid utkontraktering för teknisk bearbetning och teknisk lagring oavsett om uppgifterna blir tillgängliga för (tagits del av) mottagaren eller inte. Grunden i svensk rätt är att uppgifter är offentliga om de inte är sekretessbelagda. Sekretess och tystnadsplikt innebär i princip ett på visst sätt avgränsat förbud för myndigheter och de som deltar i myndigheters verksamhet att *lämna ut* och *röja sekretessbelagda uppgifter*, vare sig det sker genom att allmän handling lämnas ut eller det sker muntligen eller på annat sätt (se prop. 1979/80:2 Del A s. 69. Jfr prop. 2008/09:150 s. 299 och 364). Sekretess och tystnadsplikt innebär att uppgifter som ska hållas hemliga *inte får röjas* (se prop. 1979/80:2 Del A s. 69). Utredningen menar dock att det i situationer som avser utkontraktering av teknisk bearbetning och teknisk lagring inte krävs att mottagaren *tagit del* av uppgifter för att de ska betraktas som röjda. Centralt är därmed inte om en tredje part genom kryptering eller pseudonymisering är förhindrad att ta del av sekretessbelagda uppgifter utan att de *lämnas ut* (se synpunker i avsnitt 10.1.4. nedan). Det råder stor oenighet gällande innebörden av vad *utlämnande* och *röjande* av sekretessbelagda uppgifter innebär vilket framhålls i avsnitt 9 i utredningen (se särskilt avsnitt 9.5). Röjandebegreppet tycks härutöver inte ges samma innebörd i situationer som omfattar digital och analog miljö (se avsnitt 10.3.1 nedan).

9. Tidigare utredningar

9.8.3 US CLOUD Act och liknande regleringaroch 8 kap. 3 § OSL

Polismyndigheten ställer sig frågande till att utredningen synes göra bedömningen att svenska myndigheter friskrivs från ansvar gällande risken för att uppgifter ska lämnas ut av en tjänsteleverantör till en utländsk myndighet. Detta eftersom det inte kan bli fråga om ett otillåtet röjande i förhållande till tredjeland när endast en risk för röjande föreligger, det vill säga om tredjelands myndigheter kräver ut uppgifterna av en anlitad tjänsteleverantör. Utredningen fokuserar på själva överföringen till tredjeland, samtidigt som det konstaterats att en uppgift är röjd även om någon inte tar del av den.[8] Internationella företag som lyder under extraterritoriell lagstiftning har otvivelaktigt åtkomst till uppgifterna, och i förlängningen således även landets myndigheter.

[8] Se sid 240 ff i utredningen.

10. En sekretessbrytande bestämmelse

10.1.4 Avtalsreglerad tystnadsplikt, kryptering och pseudonymisering

Polismyndigheten anser att det skulle få oöverskådliga effekter och näst intill omöjliggöra myndigheters elektroniska kommunikation om all trafik där kryptering används som säkerhetsåtgärd för konfidentialitet, både inom förvaltningen och mellan förvaltningen och kommersiella aktörer, skulle betraktas som röjd. Utredningens syn stämmer inte överens med tidigare gjorda bedömningar på området, exempelvis i 3 kap 5 § andra stycket säkerhetsskyddsförordningen[9].

Utredningen tycks göra bedömningen att uppgifter är röjda så fort de lämnats ut, det vill säga så fort de lämnat en myndigheten som en generell regel, utan hänsyn tagen till vilken typ av information det är fråga om och utan hänsyn tagen till krypteringens kvalitet. Ställningstagandet leder till orimliga konsekvenser som exempelvis att av försvarsmakten godkända kryptosystemen som säkerhetsskyddsförordningen kräver vid överföring av säkerhetsskyddsklassificerade uppgifter inte längre kan användas utan att uppgifter ska betraktas som röjda. Det måste finnas ett mått av rimlighet för att uppgifter i förväg ska behöva betraktas som röjda.

Frågor som rör elektronisk kommunikation och integritetsskydd tycks inte beröras i utredningen varför Polismyndigheten efterlyser en analys av hur exempelvis e-dataskyddsdirektivet, 2002/58/EU, förhåller sig till utredningens ställningstaganden och förslag.

10.3.1 Tillämpningsområdet

Mot bakgrund av att reglerna för arkivhandlingar idag till stor del är teknikneutrala anser Polismyndigheten att det inte finns skäl att ha olika regler för utkontraktering av it-drift med elektroniska handlingar och utkontraktering av förvaring av fysiska handlingar. Detta borde beaktas i utredningen.

10.3.4 En intresseavvägning

I det fall förslaget införs vill Polismyndigheten framhålla vikten av att myndigheterna får stöd och vägledning gällande den föreslagna intresseavvägningen, vilket föreslås i avsnitt 12.4 av utredningen. Intresseavvägningen kommer ställa höga krav på verksamhetsutövarens förmåga att utföra en korrekt och enhetlig riskbedömning.

Genom OSL har lagstiftaren vägt huvudregelns offentlighet mot intresset av att belägga en viss specifik uppgift med sekretess och också avgöra hur starkt detta sekretesskydd ska vara. Då lagstiftaren redan gjort en intresseavvägning

---

[9] Där anges att om säkerhetsskyddsklassificerade uppgifter ska kommuniceras till ett informationssystem utanför verksamhetsutövarens kontroll ska uppgifter skyddas med hjälp av kryptografiska funktioner som har godkänts av Försvarsmakten. Regleringen innebär en avvägning av informationens skyddsvärde – säkerhetsskyddsklassificerade uppgifter – mot graden av skydd – försvarsmaktsgodkänt krypto. Syftet med denna reglering måste också rimligtvis vara att en bedömning gjorts att kryptosystem som godkänts av Försvarsmakten håller en sådan kvalitet att uppgifterna som förmedlas med användning av kryptot inte automatiskt röjs.

gällande vilka uppgifter som är värda att skydda med sekretess är det svårt att överblicka konsekvenserna av ett så omfattande och generellt sekretessundantag som det som utredningen föreslår och hur det ska tolkas. Risken är att detta kommer att styras av olika myndighetsföreskrifter vilket kan leda till både osäkerhet och bristande enhetligheten i den offentliga verksamheten.

13.5.8 Allmänna handlingar och arkivering

Polismyndigheten noterar att det i utredningen saknas väsentliga kartläggningar av de rättsliga förutsättningarna för myndigheters utkontraktering av it-drift utifrån författningarna som gäller hanteringen av allmänna handlingar. Regelverket gällande allmänna handlingar hade behövt genomlysas med samma noggrannhet som exempelvis reglerna för statliga myndigheters informationssäkerhet.[10] Idag är merparten av de allmänna handlingarna som finns hos en myndighet elektroniska och vid en utkontrakterad it-drift kommer stora mängder allmänna handlingar att ingå i det som driftas.

Polismyndigheten ser att det kan bli mycket svårt att säkerställa olika krav gällande allmänna handlingar vid utkontraktering av teknisk bearbetning och teknisk lagring som inte berörts av utredningen. Av relevans är här exempelvis *Riksarkivets föreskrifter (RA–FS 1991:1) och allmänna råd om arkiv hos statliga myndigheter (ändrade 2019:2*) som gäller i tillämpliga delar för handlingar som myndigheter framställer eller förvarar för annan myndighets räkning för teknisk bearbetning eller teknisk lagring. I föreskrifterna ställs bland annat olika krav på myndigheter som överlåter framställning, teknisk bearbetning eller teknisk lagring av handlingar till en annan myndighet eller till en enskild – dvs. vid utkontraktering.[11] Vid en utkontraktering behöver den myndighet som äger uppgifterna ställa ett antal krav på kvalitet på hårdvaran, hantering, förvaring och skydd etc.[12]

Ett annat exempel är *Riksarkivets föreskrifter (RA-FS 2009:1) och allmänna råd om elektroniska handlingar (upptagningar för automatiserad behandling)* som ställer tydliga krav på situationer när man upphandlar program eller tjänster för utveckling eller drift av ett system liksom när man överlåter teknisk framställning, bearbetning eller bevarande av elektroniska handlingar till en annan myndighet eller enskild. Vid utkontraktering av it-drift i utredningens mening kan det exempelvis bli svårt att uppfylla relevanta krav i en upphandling såsom tillgång till program och dokumentation för tillämpningen av föreskrifterna eller skyldigheten för leverantören att följa de bestämmelser som är tillämpliga och ta emot arkivmyndighet för inspektion.[13] Myndigheten får inte överlåta prövningen av utlämnande av allmänna handlingar åt annan. Vidare kan det bli svårt för myndigheterna att uppfylla krav om rutiner och åtgärder inom informationssäkerhetsområdet för att säkerställa bevarande av elektroniska handlingar samt att genomföra riskanalyser innan driftsättning eller in-

[10] Jfr avsnitt 6.3.2

[11] Se även, PM Arkivbildning i delade system som Riksarkivet tagit fram under 2020 som stöd för myndigheterna

[12] Se Riksarkivets föreskrifter (RA-FS 2019:2).

[13] Riksarkivets föreskrifter (RA-FS 2009:1) och allmänna råd om elektroniska handlingar (upptagningar för automatiserad behandling), 1 kap. 9 och 10 §§.

nan uppdrag ges till annan myndighet eller enskild för att bedöma behovet av säkerhetsrutiner.[14]

I *Riksarkivets föreskrifter (RA-FS 2013:4) och allmänna råd om arkivlokaler* krav på att om en myndighet lämnar arkiv (vilket även omfattar elektroniska handlingar) för förvaring hos en kommunal myndighet eller hos en enskild ska myndigheten genom skriftlig överenskommelse säkerställa att den som förvarar arkivet tillämpar Riksarkivets föreskrifter.[15]

För att underlätta för myndigheterna har Riksarkivet tillsammans med MSB tagit fram en *Vägledning för fysisk informationssäkerhet i it-utrymmen.* I vägledningen ställs krav på att Riksarkivet ska få yttra sig om it-utrymmen där allmänna handlingar ska förvaras. Riksarkivet har även rätt att inspektera förvaringen oavsett arkivets fysiska placering. Någon diskussion om kravställning på tjänsteleverantörer vid utkontraktering av teknisk bearbetning och teknisk lagring finns inte i utredningen.

Konsekvenser för Polismyndigheten

Polismyndigheten ser inte att ett genomförande av förslagen kommer att öppna upp för omfattande utkontraktering av teknisk bearbetning och teknisk lagring då intresset av sekretess och dataskydd till största del troligen kommer väga tyngre än utkontraktering. Detta mot bakgrund av att en avvägning till stor del redan är gjord av lagstiftaren genom OSL samt begränsas av EU-rätten. Polismyndigheten ser dock att risken för ökad rättsosäkerhet kan öka arbetsbördan för myndigheten vid olika bedömningar gällande sekretess och dataskydd.

Detta yttrande har beslutats av rikspolischef Anders Thornberg efter föredragning av juristen Maria Wiberg.

POLISMYNDIGHETEN

Anders Thornberg

Ida Forss
på uppdrag av Maria Wiberg

Kopia till:

Justitiedepartementet (PO)
Arbetstagarorganisationerna
Rikspolischefens kansli

[14] Riksarkivets föreskrifter (RA-FS 2009:1) och allmänna råd om elektroniska handlingar (upptagningar för automatiserad behandling), 6 kap. 1 och 3 §§.
[15] Riksarkivets föreskrifter (RA-FS 2013:4) och allmänna råd om arkivlokaler, 1 kap. 2 §.