Sveriges Kommuner och Regioner

YTTRANDE

Vårt ärendenr:
21/00160

2021-04-23

Ert dnr:
I2021/00342

Sektionen för digitalisering och inköp
Lotta Nordström

Infrastrukturdepartementet
103 33 STOCKHOLM

Säker och kostnadseffektiv it-drift SOU 2021:1

Sveriges Kommuner och Regioner (SKR) har beretts möjlighet att lämna yttrande på delbetänkandet av IT-rättsutredningen SOU 2021:1. SKR lämnar, utifrån de aspekter som följer av vårt uppdrag, följande synpunkter på det remitterade underlaget.

Det är endast en del av betänkandet som ligger till grund för förslag till lagändringar. I remissvaret fokuserar SKR huvudsakligen på dessa frågor men vissa frågor som rör bedömningar i förhållande till dataskyddsregelverket vill SKR ändå kommentera, vilket görs i bilaga till detta remissyttrande.

Sammanfattning (SKR:s sammanfattande synpunkter)

SKR delar utredningens syn på att en sekretessbrytande bestämmelse behövs men att ordalydelsen av den föreslagna bestämmelsen i OSL bör förenklas och förtydligas. SKR lämnar ett förslag på en sådan formulering.

Den föreslagna bestämmelsen bör inte innefatta myndigheter då detta krockar med den befintliga formuleringen i 11:4a OSL.

SKR delar inte it-driftsutredningens slutsats att det av lagtexten går att utläsa att utlämning alltid innebär att en sekretessgräns passeras.

SKR håller inte med utredningen om att det går att sätta likhetstecken mellan utlämnande och röjande på sådant sätt som utredningen gör gällande.

SKR menar att kryptering är en sådan åtgärd som innebär att uppgifter kan lämnas ut till och hanteras av en obehörig utan att uppgiften ska anses vara röjd.

SKR utgår från att det föreslagna begreppet teknisk bearbetning och tekniskt lagring i den sekretessbrytande bestämmelsen även inkluderar alla tjänster som kan ingå i tillhandahållande av it-drift.

SKR anser att det behöver förtydligas att den sekretessbrytande bestämmelsen även kan tillämpas i förhållande till underleverantörer till det företag som en myndighet anlitar.

Slutligen kommenterar SKR utredningens analys av dataskyddslagstiftningen i en bilaga till remissvaret.

Sveriges Kommuner och Regioner
Post: 118 82 Stockholm, *Besök:* Hornsgatan 20
Tfn: växel 08-452 70 00, *Fax:* 08-452 70 50
Org nr: 222000-0315, info@skr.se, www.skr.se

Allmänna synpunkter

SKR ser ett stort behov av ett helhetsperspektiv på informationshantering för såväl kommuner, regioner och stat, oavsett om informationen finns i analog eller digital form, och oavsett om den skapades igår, skapas idag eller kommer att skapas i morgon. Det behövs en enhetlig syn inom den statliga, regionala och kommunala förvaltningen på tillämpningen av offentlighets- och sekretesslagen, dataskyddsförordningen och förutsättningarna för överföring av personuppgifter till tredje land.

SKR ser övervägande positivt på utredningens förslag om införande av en sekretessbrytande bestämmelse vid utkontraktering av it-drift. Tillsmannans med bestämmelsen om tystnadsplikt för företag eller annan enskild som trädde i kraft den 1 januari 2021 och förslaget om inskränkningen av meddelarfriheten för dessa aktörer blir reglerna om utkontraktering av it-drift tydligare.

Av utredningens direktiv (Bilaga 1 s. 357 (bakgrund) och 368 (uppdraget att utreda rättsliga förutsättningar för utkontraktering till privata aktörer) framgår att det bland myndigheterna råder osäkerhet angående de rättsliga förutsättningarna för utkontraktering. Bland annat om när en uppgift ska anses röjd enligt sekretesslagstiftningen, men också när det gäller personuppgifter som kan komma att föras över till tredje land. Utredningen fick därför i uppdrag att analysera och klargöra de rättsliga förutsättningarna för offentliga myndigheters möjligheter att anlita privata leverantörer. Även om utredningen gjort ett antal klargöranden som t.ex. avseende 8 kap 3 § offentlighets- och sekretesslagen (2009:400) anser SKR att det fortfarande finns betydande oklarheter som hade behövt klargöras och där utredningens resonemang tyvärr skapat ytterligare frågor. Dessa frågor rör bland annat utredningens slutsatser att

- utlämnande alltid innebär att uppgifter röjs,
- kryptering aldrig är en skyddsåtgärd som innebär att uppgifter inte röjs, eller
- krypterade personuppgifter inte får överföras till tredje land om inte rättsordningen i det aktuella landet erbjuder ett skydd som är väsentligen likvärdigt med det skydd som garanteras genom artiklarna 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna (stadgan).

Det är av stor vikt för SKR:s medlemmar att de regler som medlemmarna är skyldiga att tillämpa är lätta att förstå och enkla att omsätta i praktiken samt är så generellt tillämpbara som möjligt. Den intresseavvägning som utredningen föreslår lägger ett stort ansvar på de offentliga aktörerna att väga olika intressen mot varandra. Detta är en komplex övning då olika storheter ställs mot varandra. Den offentliga aktörens intressen av att använda tjänsterna mot uppgifternas art och omfattning, intresset som sekretessen ska skydda, eventuell tystnadsplikt hos mottagaren och möjligheterna att lagföra brott mot sådan tystnadsplikt m.m.

Bedömningarna ställer höga krav på kompetens och erfarenhet hos den offentliga aktörens medarbetare, vilket kan vara svårt för till exempel små kommuner. Om de offentliga aktörerna inte får mer ledning i hur de bör resonera vid intresseavvägningen finns det risk för att avvägningen inte blir den slutliga kontrollstation som garanterar att utkontraktrering får ske, eller inte får ske.

Synpunkter per avsnitt och förbundets ställningstagande i kronologisk ordning

När det gäller de olika avsnitten i betänkandet har SKR följande synpunkter.

1.1 Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)

Utredningens förslag	*SKR:s förslag*
2 a §	2 a §
Sekretess hindrar inte att en uppgift lämnas ut till ett företag eller en annan enskild *eller till en annan myndighet som har i uppdrag* att *utföra endast teknisk bearbetning eller teknisk lagring av de uppgifter* som lämnas ut för den utlämnande myndighetens räkning.	Sekretess hindrar inte att en uppgift lämnas ut till ett företag eller en annan enskild *(tjänsteleverantör)* för att enbart teknisk bearbeta eller teknisk lagra uppgiften som lämnas ut för den utlämnande myndighetens räkning.
En uppgift ska inte lämnas ut om det intresse som sekretessen ska skydda har företräde framför intresset av att uppgiften lämnas ut.	En uppgift ska inte lämnas ut om det intresse som sekretessen ska skydda har företräde framför intresset av att uppgiften lämnas ut.

Skälen till SKR:s förslag: SKR ifrågasätter om det verkligen behövs en sekretessbrytande bestämmelse i förhållande till myndigheter eftersom det redan finns en bestämmelse om överföring av sekretess i 11 kap. 4 a § OSL.

I betänkandet saknas resonemang kring möjligheten för företag att använda underleverantörer vid utförandet av uppdrag att endast tekniskt bearbeta eller tekniskt lagra uppgifter. Det är inte ovanligt att företag, andra enskilda eller myndigheter anlitar underleverantörer för att helt eller delvis utföra uppdrag som består i att endast tekniskt bearbeta eller tekniskt lagra uppgifter, (jfr Prop. 2019/20:201 s. 10 f.). Myndigheten måste alltså i sin prövning av om utkontraktering kan ske även beakta att en eller flera underleverantörer kan komma att ges tillgång till myndighetens uppgifter. I 3 § lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter förtydligades detta uttryckligen i lagtexten.

Eftersom det saknas resonemang kring möjligheten att anlita underleverantörer i betänkandet uppstår en oklarhet över om det är tillåtet med stöd av bestämmelsen. Det är SKR:s uppfattning att möjligheten att anlita underleverantörer inte bör eller ska inskränkas eftersom det kan medföra ytterligare svårigheter och fördyringar för medlemmarna vid upphandling av dessa typer av tjänster.

SKR föreslår att bestämmelsen förtydligas på så sätt att det inte råder någon tvekan om att det fortfarande ska vara möjligt för leverantörer att anlita underleverantörer vid fullgörandet av dessa typer av uppdrag. Det kan göras genom ett förtydligande i lagtexten som SKR föreslår, genom ett nytt stycke liknande 3 § lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter eller ett förtydligande i kommentaren. Se vidare SKR:s synpunkter i anslutning till avsnitt 10.3 och 15 nedan.

8.9 Röjandebegreppet

8.9.1 Lagtexten

SKR delar inte it-driftsutredningens slutsats att utlämning alltid innebär att en sekretessgräns passeras. Av definitionen av sekretess framgår att sekretess är ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt.

Det innebär att röjande kan ske genom utlämnande. Det innebär dock inte att utlämnande alltid innebär ett röjande.

SKR menar att om ett utlämnande sker mot bakgrund av en sekretessbrytande bestämmelse, en bestämmelse om överföring av sekretess eller om uppgiften omfattas av en primär sekretessbestämmelse hos mottagaren så är den sekretessbelagda uppgiften inte röjd.

En uppgift är inte heller röjd om uppgiften utlämnas efter en skadeprövning som konstaterar att ingen skada som sekretessen är avsedd att skydda uppstår – då föreligger nämligen ingen sekretess.

Att röja en uppgift måste rimligen avse att lämna en uppgift till något eller någon som är obehörig att ta del av uppgiften. Då blir det också rimligt att det förtydligas att sekretess är ett förbud att röja. Därmed är inte röja ett neutralt uttryck som kan jämställas med att lämna ut. Detta synsätt vinner också stöd av 2 kap. 3 § säkerhetsskyddsförordningen (2018:658) och 4 kap 1 § patientdatalagen (2008:355). Uppgifter är enligt dessa regelverk inte röjda bara för att obehöriga har potentiell tillgång till dem. Det krävs att det tillkommer ytterligare omständigheter som visar om uppgifterna röjts. Det stämmer också med synsättet att röjande kan ske även inom en myndighet, t.ex. mellan olika nämnder inom en region eller kommun – något som it-

driftsutredningen varit tvungen att bortse från för att bedömningen ska kunna tillämpas.

Av 18 kap 9§ offentlighets- och sekretesslagen framgår bland annat sekretess för uppgift om chiffer, kod eller liknande metod, om det kan antas att syfte att underlätta befordran eller användning i allmän verksamhet av uppgifter utan att föreskriven sekretess åsidosätts. Bestämmelsen tar sikte på situationer när sekretessbelagda uppgifter hanteras av obehöriga utan att föreskriven sekretess åsidosätts. Bestämmelsen förutsätter alltså att det måste finnas metoder och situationer där uppgifter lämnats eller hanteras av obehöriga utan att de sekretessbelagda uppgifterna är röjda.

It-driftsutredningen använder uttryck som att uppgifter kan ”betraktas som röjd”, ”ska ses som röjd” ”betraktas som utlämnad” Detta uttryckssätt finner inget stöd i offentlighets- och sekretesslagen (2009:400) (OSL). Från lagens synvinkel är en uppgift antingen utlämnad eller inte utlämnad, röjd eller inte röjd. Rekvisitet ”betraktas” eller ”ses” tar sikte på ett hanterandeförfarande. Det vill säga även om en uppgift i objektiv mening inte är röjd kan omständigheterna vara sådana att en verksamhetsutövare där uppgifterna förekommer ändå måste vidta åtgärder för att minska risken för skada om det skulle vara så att uppgifterna ändå finns tillgängliga för obehöriga.

Det är således – som i fallet med transportstyrelsen – så att även om en domstol kommer fram till slutsatsen att uppgifterna inte är röjda i straffrättsligt hänseende så kan en myndighet behöva betrakta uppgifterna som röjda oavsett om uppgifterna röjts eller inte eftersom konsekvenserna av om uppgifterna kommit obehöriga till del utan att man kan se tydliga tecken på det är så allvarliga att myndigheten inte kan ta risken att eventuell skada uppstår. OSL innehåller inga hanteranderegler om hur en myndighet ska agera om en sekretessbelagd uppgift misstänks ha röjts. Detta är något som varje myndighet själva har att bestämma om inte lagstiftaren ställt särskilda krav som till exempel i 2 kap. 10 § säkerhetsskyddsförordningen (2018:658), 18 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster eller Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av it-incidenter för statliga myndigheter (MSBFS 2020:8).

8.10 Våra samlade bedömningar

Av definitionen av sekretess framgår att röjande kan göras genom utlämnade av allmän handling. Det är inte samma sak som att ett utlämnande är en form av röjande.

SKR menar således att det inte går att sätta likhetstecken mellan utlämnande och röjande på sådant sätt som utredningen gör gällande. Det kan förekomma utlämnande som inte innebär att en uppgift röjs för obehörig.

Ett synsätt som medför att varje utlämnande innebär ett röjande skulle dessutom leda till att alla tjänstepersoner som lämnar sekretessbelagda uppgifter till andra myndigheter där uppgifterna också är sekretessbelagda och där uppgifterna behövs för verksamheten i objektiv mening skulle göra sig skyldig till brott mot tystnadsplikten enligt 20 kap 3 § brottsbalken. Tjänstepersonen röjer en uppgift som personen är pliktig att hemlighålla enligt lag.

9.8.2 Teknisk bearbetning eller teknisk lagring

SKR vill framhålla att bestämmelsen om överföring av sekretess för enbart teknisk bearbetning och teknisk lagring (11 kap. 4 a § offentlighets- och sekretesslagen (2009:400) är att det ska vara tydligt att sekretess även gäller hos den mottagande myndigheten. Det vill säga så att uppgiften inte ska bli röjd genom den tekniska bearbetningen och lagringen samt att tystnadsplikt ska råda och meddelarfriheten kan inskränkas även hos den behandlande myndigheten.

Det är således inte – som utredningen gör gällande – en förutsättning för att en bestämmelse om överföring av sekretess ska tillämpas att den överlämnande myndigheten röjt uppgiften genom överlämningen. Utan tvärt om så att bestämmelsen om överföring av sekretess finns för att uppgifterna inte ska bli röjda.

9.9 När är en uppgift röjd i den mening som avses i straffbestämmelsen om vårdslöshet med hemlig uppgift enligt NJA 1991 s. 103

SKR anser i likhet med arbetsdomstolen i AD 2019 nr 15 att principen i NJA 1991 s. 103 om när sekretessbelagda uppgifter är röjda även kan tillämpas på digitala uppgifter och att prejudikatet inte är begränsat till uppgifter dokumenterade i pappershandlingar. Något särskilt skäl till varför prejudikatet kan tillämpas på fysiska pappershandlingar framförs inte av utredningen och SKR menar att principerna måste kunna tillämpas oavsett om informationen finns i digital eller analog form.

10 En sekretessbrytande bestämmelse

10.1 Utkontraktering och röjande och 10.13 En utkontraktering innebär att uppgifterna lämnas ut och därmed röjs

Som framgår av ovanstående kommentarer delar inte SKR bedömningen att utlämning är en form av röjande eftersom det kan förekomma att uppgifter lämnas ut utan att de för den skull är röjda i offentlighets- och sekretesslagens mening i vart fall om mottagaren är en myndighet där uppgiften fortsatt omfattas av sekretess. Så borde även vara fallet om mottagaren av uppgifterna är behörig och uppgifterna är rättsligt skyddade även hos mottagaren. Det kan också vara så att uppgifterna är skyddade av kryptering vilket torde innebära att de kan vara utlämnade utan att vara röjda.

10.1. 4 Avtalsreglerad tystnadsplikt, kryptering och pseudonymisering

SKR har uppfattningen att kryptering är en sådan åtgärd som innebär att uppgifter kan lämnas ut till och hanteras av en obehörig utan att uppgiften röjs dvs. utan att föreskriven sekretess åsidosätts. Detta synsätt delas också av rättsordningen exempelvis genom 18 kap. 9 § offentlighets- och sekretesslagen (2009:400) och Försvarsmaktens föreskrifter om signalskyddstjänsten (FFS2021:1), jfr bilaga 1.

Om utredningens synsätt skulle råda så skulle det innebära att även fysiska handlingar skulle vara utlämnade och därmed också röjda om en myndighet hyr lokaler av en annan myndighet eller av en privat hyresvärd eftersom det alltid kommer att finnas en teoretisk och praktisk möjlighet för hyresvärden att ta del av uppgifterna då det sker i dennes lokaler. Det kan även tänkas att uppgifter som finns i ett kassaskåp eller en portfölj teoretiskt kan låsas upp av en obehörig även om uppgifterna befinner sig i utrymmen som ägs av eller kontrolleras av myndigheten.

SKR vill framhålla betydelsen av att inte tillämpa olika principer beroende på om uppgifter finns i analog eller digital form, och oavsett om uppgifter skapades igår, skapas idag eller kommer att skapas i morgon. Det är naturligt att olika skyddsåtgärder måste tillämpas beroende på uppgifternas form, men det är olyckligt att i sin helhet underkänna skyddsåtgärder för uppgifter i en viss form och samtidigt acceptera skyddsåtgärder för en annan form.

Det är istället rimligt att kunna tillämpa NJA 1991 s. 103 även i en digital miljö och då vid bedömningen av om en uppgift är röjd eller inte titta på om det finns några omständigheter som tyder på att uppgifterna röjts av en obehörig. Det kan göras genom exempelvis andra kompletterande skyddsåtgärder som loggning med mera.

I avsnittet synes utredningen blanda ihop skillnaden mellan personuppgiftshantering och sekretess enligt offentlighets- och sekretesslagen (2009:400). De JO-ärenden som utredningen hänvisar till handlar om utlämnande av personuppgifter till tredje land och bedömningen utgår från att uppgifter röjs oavsett om de krypteras eller pseudonymiseras. Pseudonymisering som kan liknas vid en sorts kryptering är inte något som brukar diskuteras i sekretessammanhang utan förekommer endast i dataskyddsförordningen.

10.2 En sekretessbrytande bestämmelse behövs

SKR delar utredningens slutsats om att en sekretessbrytande bestämmelse behövs i förhållande till företag och enskilda (tjänsteleverantörer) I förhållande till myndigheter blir det otydligt med en sekretessbrytande bestämmelse, då en sådan bestämmelse riskerar att undergräva den sekretess som redan råder enligt 11 kap, 4a§ OSL. SKR förslår därför att myndigheter tas bort från bestämmelsens tillämpningsområde.

Grunden för behovet är emellertid inte att SKR anser att det idag saknas möjlighet att anlita externa leverantörer för it-drift utan för att det innebär en lättare hantering för SKR:s medlemmar. Det skapar mindre osäkerhet om avtalen om konfidentialitet och

tystnadsplikt är tillräckliga och minskar behovet av att göra skadeprövningar i den mån det är tillämpligt.

10.3 Den sekretessbrytande bestämmelsens utformning

SKR utgår från att begreppet teknisk bearbetning och tekniskt lagring även inkluderar alla tjänster som kan ingå i tillhandahållande av it-drift.

SKR anser att det behöver förtydligas att den sekretessbrytande bestämmelsen även kan tillämpas i förhållande till underleverantörer till det företag som en myndighet anlitar.

Utredningen har inte funnit några skäl att begränsa den sekretessbrytande bestämmelsen i förhållande till myndigheter men samtidigt inte resonerat om hur det påverkar bestämmelsen om överföring av sekretess enligt 11 kap. 4 a § offentlighets- och sekretesslagen (2009:400). SKR menar att bestämmelsen om överföring av sekretss i förhållande till myndigheter gör behovet av en sekretessbrytande bestämmelsen i förhållande till myndigheter överflödigt och riskerar enbart att skapa större förvirring.

Den intresseavvägning som utredningen föreslår lägger ett stort ansvar på de offentliga aktörerna att väga olika intressen mot varandra. Detta är en komplex övning då olika storheter ställs mot varandra. Den offentliga aktörens intressen av att använda tjänsterna mot uppgifternas art och omfattning, intresset som sekretessen ska skydda, eventuell tystnadsplikt hos mottagaren och möjligheterna att lagföra brott mot sådan tystnadsplikt m.m.).

Bedömningarna ställer höga krav på kompetens och erfarenhet hos den offentliga aktörens medarbetare, vilket kan vara svårt för till exempel små kommuner. Om de offentliga aktörerna inte får mer ledning i hur de bör resonera vid intresseavvägningen finns det risk för att avvägningen inte blir den slutliga kontrollstation som garanterar att utkontraktrering får ske, eller inte får ske.

Sveriges Kommuner och Regioner

Anders Knape
Ordförande

Särskilt yttrande lämnades av Socialdemokraterna, se Bilaga 1.

Bilaga till SKR svar på Säker och kostnadseffektiv it-drift SOU 2021:1

7 Dataskydd

7.3.3 Personuppgiftsansvarets innebörd vid anlitande av ett personuppgiftsbiträde

SKR håller inte med utredningen om att det i artikel 28 och skäl 81 i Dataskyddsförordningen går att utläsa en definitiv omsorgsplikt där den personuppgiftsansvarige är skyldig till att behöva utreda under vilka förutsättningar ett personuppgiftsbiträde har möjlighet att efterleva sina skyldigheter enligt förordningen. Det som framgår dataskyddsförordningen är att endast person-uppgiftsbiträden som ger tillräckliga garantier ska användas. Men inte hur personuppgiftsansvarig ska kontrollera detta.

Det som framgår som ett krav i skäl 81 är enbart att personuppgiftsbiträdet behöver lämna tillräckliga garantier om att personuppgiftsbiträdet kan genomföra lämpliga organisatoriska och tekniska skyddsåtgärder. Med det sagt är det fortfarande möjligt att, som utredningen själv konstaterar, att ta tredje lands lagstiftning i beaktande i de fall där den personuppgiftsansvarige finner skäl att tvivla på personuppgiftsbiträdets garantier. Att det föreligger ett visst ansvar för den personuppgiftsansvarige att vid behov kontrollera personuppgiftsbiträdet framgår även av principen om ansvarsskyldighet i artikel 5.2 Dataskyddsförordningen. Däremot enligt SKR:s mening medför själva anlitandet av ett personuppgiftsbiträde som verkar under tredje lands lagstiftning inte i sig en skyldighet för den personuppgiftsansvarige att behöva genomföra en analys av det tredje landets lag. Detta ansvar bör istället ligga på personuppgiftsbiträdet, som är den som har ett uttalat ansvar enligt förordningstexten på att kunna lämna tillräcklig garantier om tekniska och organisatoriska skyddsåtgärder. Och för att ett personuppgiftsbiträde ens ska ha en möjlighet att kunna lämna dessa garantier, så bör det vara biträdets ansvar att tillse att det tredje lands lagstiftning som biträdet är bundet av tillåter att dessa garantier är de facto möjliga att lämna till den personuppgiftsansvarige i den omfattning som Dataskyddsförordningen kräver. Om biträdet felaktigt har lämnat sådana garantier exempelvis genom att bortse från det tredje landets lagstiftning när de lämnar sina garantier, bör ansvaret för denna felaktighet ligga på personuppgiftsbiträdet och inte på den personuppgiftsansvarige.

7.3.3 Reglering av inbördes ansvar och funktioner

SKR delar inte utredningens syn på att en personuppgiftsansvarig kan ses som delansvarig enligt artikel 28.3 i förordningen enbart för att den personuppgiftsansvarige har haft skäl att misstänka att personuppgiftsbiträdet inte följer den ansvariges instruktioner. Det är först i det fallet att en personuppgiftsansvarig har haft vetskap om att personuppgiftsbiträde inte följer den

ansvariges instruktioner och därefter inte vidtagit åtgärder som det kan bli fråga om ett ansvar även för den personuppgiftsansvarige i SKR:s mening.

7.4.5 Överföring som omfattas av lämpliga skyddsåtgärder

Utredningen har i detta avsnitt bortsett ifrån användarfall 2: Transfer of pseudonymised Data, i utredningens genomgång av de rekommendationer som EDPB lämnat den 10 november 2020 (s. 220 f).

-

7.4.8 Rättsläget avseende överföring av personuppgifter till USA

SKR hade i denna del önskat ett utförligare och klargörande resonemang. EU-domstolen i *Facebook Ireland och Schrems* resonerar inte kring tekniska åtgärder.

De lämpliga skyddsåtgärder som räknas upp i artikel 46.2 och 46.3 dataskyddsförordningen är enbart administrativa och organisatoriska. Det är emellertid inte en uttömmande uppräkning av möjliga skyddsåtgärder som kan tillämpas i dessa situationer. Skäl 109 i dataskyddsförordningen öppnar upp för att använda *ytterligare skyddsåtgärder* som kan vara tekniska.

EU-domstolen i *Facebook Ireland och Schrems* gjorde sin bedömning enbart i förhållande till administrativa och organisatoriska åtgärder som ytterligare skyddsåtgärder. EU-domstolen kom till slutsatsen att administrativa och organisatoriska åtgärder inte kan anses tillräckliga mot bakgrund av amerikansk underrättelselagstiftning. Tekniska åtgärder såsom exempelvis kryptering har inte beaktats av domstolen då detta inte varit föremål för avgörandet. EU-domstolen påpekar emellertid (stycke 133) att beroende på den situation som råder i ett visst tredje land kan det vara nödvändigt att vidta ytterligare åtgärder för att säkerställa att skyddsnivån iakttas.[1]

Europeiska dataskyddstyrelsen påpekar i sitt utkast till rekommendation att avtalsrättsliga och organisatoriska åtgärder i regel inte räcker för att hindra de offentliga myndigheterna ett tredjeland från att komma åt personuppgifter. Europeiska dataskyddsstyrelsen framhåller att det kommer att finnas situationer där endast tekniska åtgärder kan hindra eller begränsa de offentliga myndigheternas åtkomst till personuppgifter i tredjelandet, i synnerhet för övervakningsändamål. I sådana situationer kan avtalsrättsliga eller organisatoriska åtgärder komplettera de tekniska åtgärderna och förstärka uppgifternas övergripande skyddsnivå, t.ex. genom att skapa hinder om de offentliga myndigheterna försöker komma åt uppgifter på ett sätt som inte är förenligt med EU:s normer (stycke 48).[2]

[1] Dom C-311/18, Data Protection Commissioner mot Facebook Ireland Ltd, Maximillian Schrems.
[2] Rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelsen med EU-nivån för skydd av personuppgifter, antagna den 10 november 2020.

Europeiska dataskyddsstyrelsen lyfter bland annat kryptering, pseudonymisering och transportkryptering som effektiva kompletterande åtgärder som i kombination med överföringsverktygen enligt artikel 46 kan uppnå en skyddsnivå som är väsentligen likvärdig med den nivå som garanteras inom EES och att det då är möjligt att gå vidare med överföringen (stycke 52 och bilaga 2) vid användning av it-driftsleverantörer som personuppgiftsbiträden.[3]

Anledningen till att dessa skyddsåtgärder får anses vara effektiva är bland annat att uppgifterna skyddas av stark kryptering och krypteringen hanteras på korrekt sätt. Resultatet innebär således enskildas personuppgifter är skyddade mot att avslöjas för myndigheter i ett tredje land som USA. Utredningens kategoriska underkännande av tekniska åtgärder i förhållande till överföring till USA motsägs i vissa delar av Europeiska dataskyddsstyrelsen och därför har skapar utredningen ytterligare oklarheter som SKRs medlemmar inte är betjänta av.

[3] A.s.

Styrelsen för SKR
2021-04-23 Dnr 21/00160

Särskilt yttrande från Socialdemokraterna

Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering (SOU 2021:1)

Dnr 21/00160

Digitalisering är vår tids största förändringsfaktor. Med den kommer nya arbetsmetoder och processer som kan ge substantiella förbättringar i kvaliteten för välfärden, ökat inflytande för invånarna och effektiviseringsvinster.

En av förutsättningarna för lyckad digitalisering är molntjänster som är säkra. Säkerhet kan ses från olika perspektiv. Stora multinationella aktörer på en globaliserad marknad kan erbjuda många tekniska fördelar som skulle kunna stärka välfärdsleveransen. Samtidigt finns det fallgropar där känsligt data från våra invånare används på otillbörligt sätt. Det kan exempelvis innefatta leverantörer som använder långtgående och aggressiv kartläggning och datainsamling s.k. ”data mining” av våra användare för att skapa underlag för påverkanskampanjer, reklam eller annonsering. Främmande makters långtgående lagstiftning kan också utgöra ett hot mot våra användare. I debatten nämns ofta amerikanska ”cloud act” som innebär en skyldighet för amerikanska leverantörer att utlämna data om andra länders invånare till amerikanska myndigheter när de så begär utan rättslig prövning i landet där tjänsten levereras. Det innefattar även möjligheten att leverantören beläggs med förbud att ens upplysa användaren om att sådant intrång har skett.

När sektorn levererar välfärdstjänster innebär det ofta att invånarna måste använda den lösning som vi väljer för att ens kunna tillgodogöra sig välfärdstjänsten full ut. En elev på en skola har inga eller ytterst små möjligheter att avstå det IT-system som skolan använder, eller en patient har inga möjligheter att påverka vilken leverantör av journalsystem som sjukhuset använder. Därför vilar det ett särdeles tungt ansvar för offentligheten att stå upp för individens rättigheter när det kommer till IT-drift. Det nuvarande förslaget till yttrande framför inte detta på ett adekvat sätt.

Vi skulle vilja att SKRs yttrande framhåller att en förutsättning för säker IT-drift är att svenska personuppgifter överlämnas på så sätt att uppgifterna inte hamnar utanför svensk eller europeisk jurisdiktion utan prövning enligt svensk eller europeisk rätt.