Kronofogden

Kronofogdemyndighetens ställningstagande

Beslutad av
Ulrika Lindén

Ansvarig organisation
Rättsavdelningen

Nr
1/21/RKF

Dokumentägare
Soheil Roshanbin

Beslutsdatum
2021-02-04

Dnr
KFM 25972-2020

Gäller fr.o.m.
2021-02-04

Ny

Kronofogdemyndighetens ställningstagande om användning av externa it-tjänster som innebär överföring eller risk för överföring av personuppgifter till tredjeland

I detta ställningstagande redogör Kronofogdemyndigheten (Kronofogden) för förutsättningarna för att myndigheten ska kunna använda sig av it-tjänster som levereras av externa leverantörer. Bakgrunden är bl.a. EU-domstolens avgörande om överföring av personuppgifter till tredjeland i mål C-311/18 (Data Protection Commissioner/Maximillian Schrems och Facebook Ireland).

När en extern it-leverantör anlitas måste det göras åtskillnad mellan situationer när en it-leverantör för över uppgifter till tredjeland med Kronofogdens godkännande eller vetskap och de situationer när det finns en risk för att det sker en överföring av personuppgifter utan myndighetens vetskap och godkännande.

När det finns en **risk** för obehörigt röjande av personuppgifterna genom överföring till myndigheter i tredjeland pga. extraterritoriell tillämpning av utländsk lagstiftning, gäller följande.

- Kronofogden kan anlita it-leverantörer inom unionen över vilka utländska ägare har ett dominerande inflytande om de i avtal garanterar att de personuppgifter som behandlas genom tjänsten inte blir föremål för överföring till tredjeland. It-leverantörens garanti ska inkludera underleverantörerna.

  Risken för obehörigt röjande av personuppgifterna genom överföring till myndigheter i tredjeland måste alltid beaktas när detta är aktuellt vid prövningen enligt dataskyddsförordningens säkerhetsbestämmelser.

När det **sker en överföring** av personuppgifter till tredjeland gäller följande.

- Kronofogden får inte överföra personuppgifter till USA med stöd av EU-kommissionens beslut om Privacy Shield enligt artikel 45.1 i EU:s dataskyddsförordning.

  Personuppgiftsöverföring till USA måste vila på andra rättsliga grunder.

- Kronofogden kan för överföring av personuppgifter till tredjeland använda sig av de av EU-kommissionen fastställda standardavtalsklausulerna. Detta förutsätter särskilda överväganden där personuppgiftsskyddet vid överföring till USA behöver kompletteras av t.ex. kontraktuella, tekniska eller organisatoriska åtgärder.

Kronofogden

Kronofogdemyndighetens ställningstagande

Beslutad av
Ulrika Lindén

Ansvarig organisation
Rättsavdelningen

Nr
1/21/RKF

Dokumentägare
Soheil Roshanbin

Beslutsdatum
2021-02-04

Dnr
KFM 25972-2020

Gäller fr.o.m.
2021-02-04

Ny

Vid en sådan överföring ska de registrerade ha ett tillräckligt skydd för sina personuppgifter och även rätt till ett effektivt rättsmedel även när personuppgiftsbehandlingen i sig inte innebär ett intrång i privatlivet. Förhandssamråd bör i svårbedömda fall ske med Integritetsskyddsmyndigheten.

- Om en överföring till tredjeland är nödvändig för att myndigheten ska kunna fullgöra en uppgift av allmänt intresse samtidigt som det saknas stöd för överföringen i artikel 46 (t.ex. standardavtalsklausulerna) får överföringen i enskilda fall göras med stöd av artikel 49 i dataskyddsförordningen.

  Riskerna för de registrerades fri- och rättigheter måste vid en sådan överföring alltid prövas enligt dataskyddsförordningens säkerhetsbestämmelser.

Beslut i detta ärende har fattats av rättschef Ulrika Lindén efter föredragning av rättsutvecklare Soheil Roshanbin. Vid den slutliga handläggningen har även enhetschef Jens Västberg deltagit.

Ulrika Lindén

Soheil Roshanbin

Kronofogden

Kronofogdemyndighetens ställningstagande

Beslutad av
Ulrika Lindén

Ansvarig organisation
Rättsavdelningen

Nr
1/21/RKF

Dokumentägare
Soheil Roshanbin

Beslutsdatum
2021-02-04

Dnr
KFM 25972-2020

Gäller fr.o.m.
2021-02-04

Ny

Rättslig promemoria

Innehåll

Kronofogden

Kronofogdemyndighetens ställningstagande

Beslutad av
Ulrika Lindén

Ansvarig organisation
Rättsavdelningen

Dokumentägare
Soheil Roshanbin

Nr
1/21/RKF

Beslutsdatum
2021-02-04

Dnr
KFM 25972-2020

Gäller fr.o.m.
2021-02-04

Ny

1 Sammanfattning

Den 16 juli 2020 meddelade EU-domstolen (EUD) dom i mål C-311/18 (Data Protection Commissioner/Maximillian Schrems och Facebook Ireland), i det följande Schrems II. Denna promemoria behandlar Kronofogdens användning av externa it-tjänster i anledning av domen.

Promemorian beskriver hur Kronofogden ska agera i situationer där det a) finns en risk för att personuppgifter överförs till tredjeland utan myndighetens vetskap eller medgivande och b) där personuppgifter överförs till tredjeland av myndigheten direkt eller av dess personuppgiftsbiträden.

2 Bakgrund

2.1 Allmänt om överföring av personuppgifter med stöd av Privacy Shield och standardavtalsklausuler

I EU:s dataskyddsförordning[1] finns det särskilda bestämmelser för hur personuppgifter får föras ut ur EU.[2] Förenklat får detta ske när skyddet för personuppgifter är väsentligen likvärdigt med skyddet inom den europeiska unionen. Detta brukar benämnas adekvat skyddsnivå. Eftersom dataskyddsförordningen är tillämplig i Kronofogdens verksamhet har myndigheten ett ansvar för att säkerställa att överföring av personuppgifter till länder utanför EU sker i enlighet med bestämmelserna i förordningen.[3]

Bedömning av vad som utgör en adekvat skyddsnivå kan i vissa fall vara svår, särskilt när det gäller utvärdering av ett annat lands rättssystem. För att förenkla informationsöverföring till s.k. tredjeland finns det därför särskilda regler i EU:s dataskyddsförordning. En av dem är EU kommissionens möjlighet att fatta ett beslut om att ett land har tillräckligt hög skyddsnivå.[4] I förhållande till USA hade kommissionen i samarbete med de amerikanska myndigheterna tagit fram en certifieringsmekanism benämnd Privacy Shield.[5] Kommissionen fattade ett beslut med innebörden att om ett amerikanskt företag ingick i Privacy Shield fanns det ett adekvat skydd för personuppgifterna. Därigenom kunde personuppgiftsansvariga inom

---

[1] 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). Se även 2–3 §§ lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.
[2] Artiklarna 44-50 i EU:s dataskyddsförordning.
[3] 1 kap. 3 § lagen om behandling av uppgifter i Kronofogdemyndighetens verksamhet.
[4] Artikel 45.1 i EU:s dataskyddsförordning.
[5] Kommissionens genomförandebeslut (EU) 2016/1250 av den 12 juli 2016 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom skölden för skydd av privatlivet i EU och Förenta staterna.

unionen överföra personuppgifter till de certifierade amerikanska företagen utan ytterligare skyddsåtgärder.

Ett annat sätt att upprätthålla adekvat skydd vid överföring till tredjeland är att den personuppgiftsansvarige ingår ett standardiserat avtal framtaget av EU-kommissionen med mottagaren. Enligt dataskyddförordningen har enbart kommissionen rätt att utforma sådana standardavtalsklausuler.[6] En personuppgiftsöverföring i enlighet med villkoren i standardavtalsklausulerna har tidigare ansetts vara en tillräcklig åtgärd för att åstadkomma en adekvat skyddsnivå.[7]

2.2 Schrems II

Rättsfallet behandlar frågor om överföring av personuppgifter från unionen till USA.[8] I målet behandlades flera frågeställningar. En huvudfråga var om beslutet om Privacy Shield stod i strid med de rättssäkerhetsgarantier som finns reglerade i EU:s dataskyddsförordning och den Europeiska unionens stadga om de grundläggande rättigheterna. En annan viktig fråga var om kommissionens beslut om utformningen av standardavtalsklausuler för dataskydd för att uppnå adekvat skydd stod i strid med EU:s rättighetsstadga.

Grunden för att ifrågasätta lagligheten av kommissionens beslut om Privacy Shield och standardavtalsklausuler var de övervakningsprogram som de amerikanska myndigheterna använder sig av.[9] I avgörandet behandlades också några närliggande frågor om dataskyddsförordningens tillämplighet och möjligheten för dataskyddsmyndigheterna att förbjuda överföring av personuppgifter. De sistnämnda frågorna redogörs inte närmare för här.[10]

EU-domstolen slog bl.a. fast följande.

- Att utformningen av de amerikanska övervakningsprogrammen ledde till att skyddet för privat- och familjeliv, skyddet för personuppgifter samt rätten till effektiva rättsmedel inskränks på ett sådant sätt att skyddet för de registrerade inte blir väsentligen likvärdig vid en överföring av personuppgifter från EU till USA,[11]

[6] Artikel 46.1 och 46.2.c i EU:s dataskyddsförordning
[7] Se https://www.imy.se/lagar--regler/dataskyddsforordningen/tredjelandsoverforing/hur-vidtar-vi-lampliga-skyddsatgarder/ senast kontrollerad den 27 januari 2021.
[8] C-311/18 - Facebook Ireland och Schrems
[9] Se punkt 55 i C-311/18 - Facebook Ireland och Schrems
[10] Se punkterna 80–90 i C-311/18 - Facebook Ireland och Schrems samt domslutet under punkt 1 och punkterna 106–121 samt domslutet under punkt 3.
[11] Se punkterna 150–200 i C-311/18 - Facebook Ireland och Schrems samt domslutet under punkt 5.

- att Kommissionen hade åsidosatt ovan grundläggande krav vid utformningen av Privacy Shield och att en adekvat skyddsnivå inte kunde uppnås på detta sätt,[12]

- att Kommissionens utformning av standardavtalsklausuler för dataskydd fortfarande kunde användas som en åtgärd för att skapa ett adekvat skydd [13] och

- att användning av standardavtalsklausulerna förutsätter att den personuppgiftsansvarige säkerställer att det finns en skyddsnivå vid överföring av personuppgifter som väsentligen är likvärdig den som finns inom EU. Det ska ske genom att den personuppgiftsansvarige vid sidan av avtalet också beaktar hur uppgifterna kommer att behandlas enligt det mottagande landets rättssystem.[14]

Rättsfallet kommer att beröras mer i avsnitt 5.1.

2.3 Problemformulering, syfte och avgränsningar

EU-domstolen har underkänt kommissionens beslut om Privacy Shield på grund av att beslutet strider mot dataskyddsförordningen tolkat i ljuset av artiklarna 7, 8 och 47 i stadgan vilket får konsekvenser för Kronofogdens verksamhet. När det gäller uppgifter som omfattas av lagen (2001:184) om behandling av uppgifter i Kronofogdemyndighetens verksamhet, dvs. kunduppgifter, överförs uppgifterna inte utanför myndighetens egna it-miljö. Däremot använder sig Kronofogden i sin verksamhet bl.a. av sociala plattformar, rekryteringsverktyg och annat verksamhetsstöd och it-verktyg som kan komma att överföra personuppgifter till tredjeland. Antalet molntjänster ökar också över tid och myndigheten bör kunna använda sig av sådana när gällande rätt medger det.

Kronofogden behöver mot bakgrund av domen kunna navigera i regelverket när myndigheten använder eller överväger att anlita externa it-tjänster som antingen överför personuppgifter till tredjeland eller där det bedöms finnas en risk för överföring av personuppgifter i strid med bestämmelserna i dataskyddsförordningen på grund av extraterritoriell tillämpning av utländsk lagstiftning.

---

[12] Ibid.
[13] Se punkterna 122–149 i C-311/-18 – Facebook Ireland och Schrems samt domslutet under punkt 2 och 4.
[14] Ibid.

Promemorians huvudsakliga syfte är att närmare klarlägga hur Kronofogden får överföra uppgifter till externa leverantörer av it-tjänster och ta ställning till hur sådana överföringar får ske.

Denna promemoria behandlar inte frågor som föranleder direkta åtgärder med anledning av EU-domstolens avgörande, dvs. inventering, dokumentation och upphörande av eventuell personuppgiftsöverföring som förlitar sig på Privacy Shield eller standardavtalsklausuler där det finns risk för rättighetsinskränkningar för de registrerade. Dessa åtgärder hanteras i särskild ordning och sker i enlighet med Integritetsskyddsmyndigheten och Europeiska dataskyddstyrelsens rekommendationer. Promemorian behandlar inte heller frågor som omfattas av offentlighets- och sekretesslagen (2009:400), frågor som ligger inom brottsdatalagens (2018:1177) eller säkerhetsskyddslagens (2018:585) område.

3 Allmänna rättsliga utgångspunkter

3.1 Grundläggande rättigheter

Var och en är gentemot det allmänna skyddad mot bl.a. avlyssning och intrång i privata meddelanden och även i övrigt mot vissa andra betydande intrång i den personliga integriteten enligt 2 kap. 6 § regeringsformen. Begränsningar i skyddet får endast göras genom lag. De måste motiveras av ett ändamål som är godtagbart i ett demokratiskt samhälle och får inte gå längre än vad som är nödvändigt för att uppnå syftet med begränsningen enligt 2 kap. 20 och 21 §§ regeringsformen.

Av artikel 8 i den Europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen), som gäller som lag i Sverige, följer vidare att var och en har rätt till respekt för sitt privat- och familjeliv och sin korrespondens. Begränsningar i denna rättighet får göras bl.a. för att förebygga oordning och brott. En begränsning får dock göras bara om den är nödvändig i ett demokratiskt samhälle. Det innebär att begränsningen måste motiveras av ett angeläget allmänt intresse och inte får gå utöver vad som behövs för att uppnå sitt syfte. Av 2 kap. 19 § regeringsformen följer att en föreskrift i lag eller annan författning inte får meddelas i strid med Sveriges åtaganden på grund av Europakonventionen.

Rätten till respekt för privatlivet slås även fast i artikel 7 i EU:s stadga om de grundläggande rättigheterna (rättighetsstadgan). Där framgår att var och en har rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer. I artikel 8 slås även fast att var och en har rätt till skydd av de personuppgifter som rör honom eller henne. Sådana uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör

honom eller henne och att få rättelse av dem. En oberoende myndighet ska kontrollera att dessa regler efterlevs. Rättighetsstadgan och Europakonventionen innehåller också i artikel 47 respektive 13 särskilda bestämmelser om rätt till ett effektivt rättsmedel vid överträdelser av de grundläggande fri- och rättigheterna.

I artikel 52 i rättighetsstadgan anges i vilken utsträckning inskränkningar får göras i de rättigheter som erkänns i stadgan. Utgångspunkten är att sådana inskränkningar endast får göras i lag och ska vara förenliga med det väsentliga innehållet i rättigheterna. Begränsningar får endast göras om de är nödvändiga och svarar mot ett allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter. Skyddet innefattar bl.a. ett krav på att behandlingen av personuppgifter måste ha stöd i en legitim och lagenlig grund och att en oberoende myndighet ska utöva tillsyn över att reglerna om behandling av personuppgifter följs. Av artikel 6.1 fördraget om Europeiska unionen följer att EU-stadgan har samma rättsliga värde som fördragen.

EU-domstolen har tidigare slagit fast att de grundläggande rättigheterna måste iakttas inte bara vid tillämpningen av genomförandelagstiftning utan också så snart nationell lagstiftning omfattas av unionsrättens tillämpningsområde (EU-domstolens dom den 26 februari 2013 i mål C-617/10 Åkerberg Fransson). Detta trots att artikel 5.1. i EU-stadgan riktar sig till medlemsstaterna endast när dessa tillämpar unionsrätten. Enligt artikel 52.3 i EU-stadgan ska de rättigheter i stadgan som motsvarar sådana som garanteras av Europakonventionen ha samma innebörd och räckvidd som i konventionen.

Vid tillämpningen av dataskyddsförordningen blir sammanfattningsvis flera rättighetskataloger aktuella för såväl skyddet för privatliv som för personuppgifter. Som nämnts förutsätter tillämpningen av dessa rättigheter också att den enskilde har en reell möjlighet att tillvarata sina intressen genom rätten till ett effektivt rättsmedel. Rättigheterna kan inskränkas i lag under vissa förutsättningar.

3.2 Extraterritoriell tillämpning av utländsk lagstiftning

Ordet jurisdiktion används först och främst för att hänvisa till en stats maktutövning över personer och egendom inom dess eget territorium. En stats jurisdiktion kan utövas genom rätten att stifta lagar och andra regler (legislativ jurisdiktion), rätten att tillämpa lagstiftningen eller skipa rätt (judiciell jurisdiktion) och rätten att verkställa åtgärder eller förverkliga beslut som fattats inom ramen för lagstiftning och rättskipning (exekutiv jurisdiktion). När det gäller exekutiv jurisdiktion är utgångspunkten i folkrätten att det råder ett förbud för stater att vidta verkställighetsåtgärder inom andra staters territorier, t.ex. använda hemliga tvångsmedel där. Detta är ett

utflöde av den s.k. territorialitetsprincipen, vilken används som grund för jurisdiktion. Tanken med territorialitetsprincipen är att ingen stat ska kränka en annan stats territoriella integritet (suveränitet). [15]

De senaste decenniernas digitala utveckling har förändrat eller möjligen försvårat tillämpningen av territorialitetsprincipen. Till skillnad från fysiska föremål och enskilda privatpersoner kan elektroniska uppgifter finnas tillgängliga i flera stater samtidigt genom direktåtkomst eller lagring. I praktiken innebär det att ett internationellt företag enligt hemlandets eller flera olika länders lagstiftningar kan vara skyldig att bereda myndigheterna i hemlandet tillgång till uppgifter var än företaget har sin verksamhet. Med andra ord tillämpas en lag utanför landets territorium, dvs. extraterritoriellt och kan komma i konflikt med lagarna i det land där verksamheten pågår.

I dataskyddsförordningen uppmärksammas problematiken med extraterritoriell tilllämpning i skäl 115. Där framgår hur överföringar som baseras på extraterritoriell tillämpningen av utländsk lagstiftning kan strida mot internationell rätt och inverkar menligt på det skydd som dataskyddsförordningen ger de registrerade. I förhållande till bestämmelserna i dataskyddsförordningen blir en överföring av personuppgifter med tillämpning av extraterritoriell lagstiftning en dold och olovlig överföring. Extraterritoriell tillämpning av utländsk lagstiftning som leder till att någon olovligen bereder sig tillgång till elektroniskt lagrade uppgifter kan i vissa fall också medföra straffansvar för dataintrång enligt 4 kap. 9 c § brottsbalken.

3.3 EU:s dataskyddsreglering

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) trädde i kraft den 25 maj 2018. Den föregicks av Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter som i Sverige hade implementerats genom personuppgiftslagen (1998:204), härefter 1995-års dataskyddsdirektiv.

Enligt artikel 288 andra stycket i fördraget om Europeiska unionens funktionssätt ska en EU-förordning ha allmän giltighet och vara till alla delar bindande och direkt tillämplig i varje medlemsstat. Till skillnad från EU-direktiv ska alltså förordningar inte implementeras i nationell rätt. I stället ska förordningsbestämmelser tillämpas av enskilda, myndigheter och domstolar som nationella författningsbestämmelser.[16]

[15] SOU 2017:89 s. 444.
[16] SOU 2017:39 s. 72–73.

Dataskyddsförordningen är alltså direkt tillämplig, men det finns möjlighet till kompletterande nationella bestämmelser. I Sverige finns kompletterande bestämmelser i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen). Det följer av 1 kap. 6 § dataskyddslagen att lagen är subsidiär i förhållande till annan lag eller förordning. Avvikande bestämmelser kan med andra ord finnas i bl.a. myndigheternas egna registerförfattningar och för Kronofogdemyndighetens del kompletteras dataskyddsförordningen och dataskyddslagen av lagen (2001:184) om behandling av uppgifter i Kronofogdemyndighetens verksamhet (1 kap. 2–3 §§ KFMdbL).

4 Risk för obehörigt röjande av personuppgifter genom överföring till myndigheter i tredjeland på grund av tillämpning av utländsk lagstiftning

4.1 Begreppet överföring

Det finns ingen legaldefinition av begreppet överföring i dataskyddsförordningen. I skälen till dataskyddsförordningen används istället begrepp som flöden av information till och från länder utanför unionen, se exempelvis skäl 101. Någon legaldefinition till begreppet överföring fanns inte heller i 1995 års dataskyddsdirektiv som i Sverige genomfördes i personuppgiftslagen (1998:204), härefter PuL. 1995-års dataskyddsdirektiv har upphävts och ersatts av dataskyddsförordningen men varken i skälen eller i bestämmelserna i sig finns det något som tyder på att begreppet överföring har fått någon annan materiell innebörd än vad som har gällt tidigare. Mot den bakgrunden får tidigare praxis och förarbeten fortfarande anses vara relevant.

I förarbetena till PuL skrevs följande om begreppet. ”Begreppet överföring – och det motsvarande uttrycket föra över – har enligt vår mening en EG-gemensam innebörd. Det verkar innebära att personuppgifter som i någon mening finns i Sverige eller i någon annan medlemsstat lämnas ut på ett sådant sätt att uppgifterna efter utlämnandet kan sägas finnas (också) i tredjeland. Att någon ges möjlighet att från tredjeland komma åt personuppgifter som finns i Sverige eller i någon annan medlemsstat via telekommunikation eller datanätverk är förmodligen ett exempel på överföring av uppgifterna till tredjeland.”.[17] Det skulle i sådant fall innebära att användning av it-tjänster utomlands där någon tillhandahåller support- eller utvecklingstjänster som förutsätter att leverantören får tillgång till uppgifter innebär en överföring.

Begreppet överföring berördes i EG-domstolens förhandsavgörande i det svenska konfirmandlärarmålet[18] (dom den 6 november 2003 i mål C-101/01). Domstolen

[17] SOU 1997: 39 s. 416
[18] RH 2004:51.

konstaterade i målet att publicering av uppgifter som en privatperson lägger ut på en webbserver inom EU inte omfattas av begreppet överföring till tredjeland. Detta även om uppgifterna är åtkomliga från hela världen.[19] Målet kretsade i huvudsak kring frågan om överföring genom publicering. Andra typer av överföring omfattades inte av domstolens prövning. Rättsfallet föranledde efter en översyn inga förslag till förändringar i personuppgiftslagen.[20]

4.2 Om överföring av uppgifter till tredjeland

Överföring av personuppgifter till länder utanför EU regleras i kapitel 5, artiklarna 44–50 i EU:s dataskyddsförordning.

Utgångspunkten enligt artikel 44 är att personuppgifter inte får föras ut ur unionen. Sådan överföring får dock ske under de förutsättningar som anges i artiklarna 45–47 och 49. Av skäl 101 framgår att det är viktigt att den skyddsnivå som fysiska personer säkerställs inom unionen genom dataskyddsförordningen inte undergrävs när personuppgifter överförs från unionen till tredjeland.

Enligt artikel 45 har kommissionen möjlighet att göra bedömning om länder utanför EU har en adekvat skyddsnivå dit personuppgifter kan överföras. I avsaknad av beslut från kommissionen kan överföring ändå ske om överföringen kompletteras med lämpliga skyddsnivåer enligt artikel 46. Inom den privata sektorn finns det en möjlighet att baserat på bindande företagsbestämmelser få överföra personuppgifter till tredjeland med tillsynsmyndighetens godkännande enligt artikel 47. Avslutningsvis kan personuppgifter trots avsaknaden av lämpliga skyddsåtgärder föras ut ur EU vid vissa undantagssituationer som framgår av artikel 49, exempelvis för att överföringen är nödvändig för viktiga skäl som rör allmänintresset eller med stöd av samtycke från den registrerade.

Artikel 48 reglerar situationen när domstolar och myndigheter i tredjeland begär tillgång till personuppgifter.

För att en behandling i form av överföring av personuppgifter till tredjeland eller en internationell organisation ska få genomföras måste även övriga bestämmelser i dataskyddsförordningen beaktas. Exempelvis måste det finnas en rättslig grund för överföringen artikel 6.1. Också de grundläggande principerna för behandling av personuppgifter i artikel 5.1 måste vara uppfyllda. Innefattar överföringen känsliga personuppgifter, måste bestämmelserna i artikel 9 följas. Innefattar överföringen

[19] EG-domstolens förhandsavgörande i det svenska s.k. konfirmandlärarmålet (dom den 6 november 2003 i mål C-101/01), p. 51–71. Se även NJA 2005 s. 361.
[20] SOU 2004:6 s. 226.

sådana personuppgifter om lagöverträdelser som avses i artikel 10, måste även bestämmelserna i den artikeln följas. Innefattar behandlingen person- eller samordningsnummer krävs det också att särskilda förutsättningar är uppfyllda (artikel 87 och 3 kap. 10 § dataskyddslagen).[21] I promemorians kontext blir det särskilt viktigt vilka krav som kan ställas på personuppgiftsbiträden enligt artikel 28 och säkerhetsbestämmelserna enligt artikel 32.

4.3 Krav på ett personuppgiftsbiträde

Enligt artikel 28.1 får den personuppgiftsansvarige endast anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra behandlingen på ett sådant sätt att behandlingen av personuppgifter inte står i strid med dataskyddsförordningen. Detta ska ske med lämpliga tekniska och organisatoriska åtgärder. I skäl 81 förtydligas att garantierna ska ges i fråga om sakkunskap, tillförlitlighet och resurser men också uppgifter om hur personuppgiftsbiträdet kommer att behandla personuppgifterna tekniskt, hur arbetet är organiserat och vilket skydd personuppgifterna har hos personuppgiftsbiträdet.

Enligt artikel 28.3 och 28.9 ska personuppgiftsbiträdets skyldigheter regleras i ett skriftligt avtal. Enligt 28.3 första stycket ska avtalet sätta ramen för personuppgiftsbiträdets behandling, förenklat uttryckt vad personuppgiftsbiträdet får göra å den personuppgiftsansvariges vägnar. Avtalet ska också reglera den personuppgiftsansvariges skyldigheter och rättigheter.

Enligt 28.3 andra stycket regleras vissa särskilda skyldigheter för personuppgiftsbiträdet i punkterna a-h. Av särskilt intresse är punkt a där personuppgiftsbiträdet enbart får behandla personuppgifter enligt instruktioner från den personuppgiftsansvarige. Undantaget från punkt a är om det krävs en särskild personuppgiftsbehandling enligt unionsrätten eller nationell lagstiftning. I tidigare granskningsärenden anmärkte Integritetsskyddsmyndigheten på brister i personuppgiftsbiträdesavtal som hade tillhandahållits av olika molntjänsteleverantörer.[22] I dessa fall var utrymmet för it-leverantören alltför vid att behandla personuppgifterna för egna ändamål och avtalen saknade reglering när tjänsteleverantören skulle ha raderat personuppgifterna.[23] En annan skyldighet som bör uppmärksammas är punkten 28.3 h där personuppgiftsbiträdet har en skyldighet att ge den personuppgiftsansvarige tillgång till all information som krävs för att visa att biträdet uppfyller sina skyldigheter enligt artikel 28, inklusive externa revisioner på personuppgiftsansvariges instruktion.

---

[21] Se Öhman, Dataskyddsförordningen (GDPR) m.m. (29 februari 2020, Juno) kommentaren till artikel 49.

[22] I aktuella fall Dropbox, Google Apps, Office 365 och Windows Azure, (Data inspektionens beslut dnr 256–2011, 1351–2012, 1475–2013, 358–2014 och 574–2011.

[23] Datainspektionens beslut (dnr 1351–2012, dnr 358-2014 och dnr 988-2014.

Liksom den personuppgiftsansvarige är personuppgiftsbiträden skyldiga att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken enligt artikel 32 i dataskyddsförordningen. Vid en olovlig personuppgiftsbehandling kan personuppgiftsbiträdet bli skadeståndsskyldig gentemot de enskilda enligt artikel 82 i dataskyddsförordningen och 7 kap. 1 § dataskyddslagen. Ett personuppgiftsbiträde kan också bli föremål för sanktionsavgift enligt artikel 83 i dataskyddsförordningen och 6 kap. 2–3 §§ dataskyddslagen. Som tidigare nämnts kan också agerandet medföra straffansvar.

Enligt artikel 28.10 i dataskyddsförordningen ska ett personuppgiftsbiträde anses vara personuppgiftsansvarig för behandlingen om den överträder dataskyddsförordningens fastställda ändamål och medel för behandlingen. Skadeståndsansvaret mot uppdragsgivaren och skyldigheten att betala sanktionsavgift m.m. kvarstår likafullt som ett biträde. Det betyder exempelvis att om ett personuppgiftsbiträde olovligen överför personuppgifter till tredjeland är det biträdet som är ansvarigt för agerandet direkt i förhållande till de registrerade.

4.4 Dataskyddssäkerhet enligt EU:s dataskyddsreglering

Enligt artikel 32 i dataskyddsförordningen ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken.

Åtgärderna ska vidtas med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter.

I artikeln ges följande exempel på lämpliga åtgärder.

a) pseudonymisering och kryptering av personuppgifter,
b) förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna,
c) förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident, och
d) ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför, i synnerhet från oavsiktlig eller olaglig förstöring, förlust

eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

Till skillnad från begreppet överföring finns det i dataskyddsförordningen tydligare uttalanden om vad som faller inom begreppet säkerhet. Som framgår av nämnda artikel omfattas exempelvis obehörig överföring eller åtkomst till personuppgifter av säkerhetsbestämmelserna.[24]

Problematiken med extraterritoriell tillämpning av utländsk lagstiftning kan i vissa fall ge den personuppgiftsansvarige skäl att anta att en viss behandling sannolikt leder till en hög risk för de registrerades rättigheter. Så kan vara fallet om någon utan tillstånd olovligen överför uppgifter till tredjeland. Under sådana förhållanden ska en konsekvensbedömning göras enligt artikel 35. Om konsekvensbedömningen visar att behandlingen skulle leda till en hög risk ska förhandssamråd ske med Integritetsskyddsmyndigheten enligt artikel 36.

4.5 Kronofogdemyndighetens övervägande om risker för obehörigt röjande

Kronofogdens bedömning: Kronofogden kan anlita it-leverantörer inom unionen över vilka utländska ägare har ett dominerande inflytande om de i avtal garanterar att de personuppgifter som behandlas genom tjänsten inte blir föremål för överföring till tredjeland. It-leverantörens garanti ska inkludera underleverantörerna.

Risken för obehörigt röjande av personuppgifterna genom överföring till myndigheter i tredjeland måste alltid beaktas när detta är aktuellt vid prövningen enligt dataskyddsförordningens säkerhetsbestämmelser.

Skäl för bedömningen: Som redan nämnts har EU-domstolen i Schrems II fastställt att utformning av de amerikanska övervakningsprogrammen innebär att skyddet för privat- och familjeliv, skyddet för personuppgifter samt de enskildas rätt till effektiva rättsmedel inskränks vid en överföring av personuppgifter från unionen till USA om inte den personuppgiftsansvarige vidtar lämpliga skyddsåtgärder.

EU-domstolens avgörande tar således sikte på behandling av personuppgifter genom *överföring* till tredjeland. Domstolen har däremot inte uttalat sig om *risker* för överföring av uppgifter enligt säkerhetsbestämmelserna i dataskyddsförordningen. Även det förslag på rekommendationer som den Europeiska dataskyddstyrelsen har remitterat, som utgår från EU-domstolens dom, handlar om personuppgifter som

[24] Se även artikel 4.12 där en personuppgiftsincident definieras och skäl 83.

överförs till tredjeland. I rekommendationerna framgår att externa it-tjänster kan användas om leverantören garanterar att personuppgifterna inte förs till tredjeland.[25] Vid analysen är det därför nödvändigt att göra en åtskillnad mellan risken för överföring och en faktisk överföring. Om uppgifter faktiskt inte har överförts men det föreligger en risk för överföring av uppgifter på grund av tillämpning av extraterritoriella lagar finns det andra regler i dataskyddsförordningen som får tillämpas.

Inledningsvis ställer dataskyddsförordningen krav på Kronofogdens val av personuppgiftsbiträde. Myndigheten måste försäkra sig om att biträdet har förmåga att leva upp till dataskyddsförordningens regelverk innan ett sådant biträde anlitas och vid behov följa upp biträdets åtaganden. Kronofogden har också ett ansvar för att tydligt reglera avtalsvillkoren för vad en leverantör får göra med uppgifterna. Detta är i synnerhet viktigt om Kronofogden inte har insyn eller har svårigheter att få insyn i tjänsteleverantörens it-miljö och personuppgiftsbehandling. I detta sammanhang kan nämnas att Europeiska dataskyddsstyrelsen för ett liknande resonemang kring frågan om hur den personuppgiftsansvarige ska agera i en situation där ett biträde kan överföra uppgifter till tredjeland. Dataskyddstyrelsen anger bl.a. att avtalet med personuppgiftsbiträdet måste reglera frågan om överföring till tredjeland för såväl biträdet som eventuella underbiträden.[26]

Kronofogden är ansvarig för den personuppgiftsbehandling som biträdet utför. Om en it-leverantör som Kronofogden har anlitat, dolt eller olovligen, överför personuppgifter till tredjeland är det leverantören som är ansvarig för överföringen med risk för skadeståndsskyldighet och sanktionsavgifter. I vissa situationer kan till och med ett sådant agerande omfattas av straffansvar för dataintrång beroende på om biträdet olovligen bereder sig ytterligare tillgång till uppgifter än vad som följer av parternas överenskommelser.

Det är mot bakgrund av vad som är känt om andra länders tillämpning extraterritoriell jurisdiktion, inte minst genom vad som har kommit fram i Schrems II, problematiskt att enbart nöja sig med de besked som lämnas från en avtalspart även med beaktande av möjligheten att beivra överträdelser av ett personuppgiftsbiträde. De påföljder som ett personuppgiftsbiträde riskerar genom en olovlig personuppgiftsöverföring utgör i och för sig ett skydd för de registrerade men Kronofogden måste även ta ett eget ansvar för de risker som är förenade med att anlita en extern it-leverantör. Den bedömningen ska ske med utgångspunkt från bestämmelserna om säkerhet enligt artikel 32.

---

[25] Se punkt 13 i recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, publicerat den 10 november 2020.
[26] Se fråga 11 i Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, publicerat den 24 juli 2020.

När en riskbedömning görs finns det ett utrymme för att bedöma vilka skador en olovlig personuppgiftsbehandling kan medföra. Det innebär att även om en uppgift inte avsiktligen hade fått överföras till tredje land finns ett visst utrymme att acceptera risken för en sådan överföring. Så kan exempelvis vara fallet med en uppgift som inte är integritetskänslig eller som i övrigt inte medför men eller skada. Sådana uppgifter kan exempelvis vara offentliga och lättillgängliga uppgifter, inte sällan publicerade på myndighetens egen hemsida, årsredovisningar, rapporter eller dylikt. Typiskt sett kan den som vill ta del av sådana uppgifter, även om det skulle handla om en utländsk myndighet, lättare inhämta dem själv än att i strid med svensk och europeisk lagstiftning förelägga ett bolag under annan jurisdiktion att överföra uppgifterna dolt. I sådana situationer finns med andra ord ingen reell risk för skada. Säkerhetsbestämmelserna ger också ett visst utrymme för att väga behovet av behandlingen mot risken med den.

För att illustrera resonemanget ges följande exempel. En myndighet vill använda sig av ett planeringsverktyg som tillhandahålls genom en extern it-tjänst i ett svenskt eller europeiskt bolag. De personuppgifter som förs över till verktyget handlar i huvudsak om namnet på medarbetare eller liknande personuppgifter som inte är känsliga ur integritetsperspektiv. Det anlitade bolaget som tillhandahåller verktyget använder sig i sin tur av en servertjänst som tillhandahålls av ett utländskt bolag med servrar i Europa. Tjänsteleverantören åtar sig enligt avtalsvillkoren att överföring av personuppgifter inte ska ske till tredjeland. Den personuppgiftsansvarige ska då bedöma risken för att personuppgifter ändå förs över till tredjeland och vilken skada som detta skulle kunna förorsaka avseende de registrerades fri och rättigheter. Tjänsten får endast användas om man utifrån detta kan bedöma säkerhetsnivån som lämplig. Om uppgifterna trots alla säkerhetsåtgärder som vidtagits olovligen förs över till tredjeland kan den registrerade inte anses lida någon större skada än om uppgifterna hade hämtats från myndigheten med stöd av offentlighetsprincipen. Om ett olovligt röjande skulle ske är tjänsteleverantören skadeståndsskyldighet gentemot de registrerade och Kronofogden. Tjänsteleverantören skulle härutöver bli skyldig att betala sanktionsavgifter och riskerar straffansvar.

5 Överföringar av personuppgifter till tredjeland baserat på bestämmelsen om adekvat skyddsnivå

5.1 Privacy Shield

Enligt artikel 45.1 får kommissionen fatta beslut om att ett land säkerställer en adekvat skyddsnivå för de registrerade. Ett sådant beslut bryter förbudet mot överföring till tredjeland enligt artikel 44. Bedömningen ska göras efter de omständigheter som anges i artikel 45.2. I huvudsak handlar bedömningen om huruvida de registrerade

har ett motsvarande skydd för uppgiftsbehandlingen som om uppgifterna hade varit kvar inom unionen.

Begreppet adekvat skyddsnivå fanns som begrepp även i 1995-års dataskyddsdirektiv och hade sin motsvarighet i 33 § PuL, där det gick framgick att det var förbjudet att till tredjeland föra över personuppgifter som är under behandling om landet inte hade en adekvat nivå för skyddet av personuppgifterna. Enligt artikel 25.6 i 1995 års dataskyddsdirektiv kunde kommissionen bedöma huruvida ett land genom bl.a. sin interna lagstiftning erbjöd de registrerade en adekvat skyddsnivå.

I beslut den 26 juli 2000 meddelade kommissionen att ett adekvatskydd kunde säkerställas genom de principer om integritetsskydd som framgick av beslutet om Safe Habor Privacy Principles.[27] Bakgrunden var att organisationer i USA enligt principen om en ”Safe Harbor” på frivillig väg kunde ansluta sig till en uppsättning dataskyddsregler som det amerikanska handelsdepartementet utformat. De ansluta företagen listades då på det amerikanska handelsdepartementets webbplats. EU-domstolen underkände dock Safe Harbor-systemet som ett sätt att nå upp till unionens krav på en adekvat skyddsnivå vid tredjelandsöverföringar (mål C-362/14 ”Schrems”).[28] EU-domstolen konstaterade att kommissionens beslut stod i strid med grundläggande rättigheter i rättighetsstadgan, men riktade också kritik mot kommissionen som vid utformningen av beslutet hade inskränkt de nationella dataskyddsmyndigheternas prövning. Beslutet förklarades därför vara ogiltigt.[29]

EU-kommissionen fattade ett nytt beslut den 12 juli 2016 med stöd av artikel 25.6 i 1995 års dataskyddsdirektiv. Beslutet fick namnet Privacy Shield och byggde i grunden på samma självcertifieringsmekanismer som Safe Harbor, men innehöll ytterligare skydd för de registrerade för att tillgodose EU-domstolens krav, bl.a. en ombudsmansmekanism.[30]

Privacy Shield var giltig med stöd av artikel 45.6 i dataskyddförordningen även efter förordningens ikraftträdande, men upphävdes den 16 juli 2020 av EU-domstolen i målet Schrems II. I huvudsak ansåg EU-domstolen på samma sätt som i tidigare mål att utformningen av de amerikanska övervakningsprogrammen innebar en inskränkning i de grundläggande rättigheterna enligt artikel 7, 8, och 47

---

[27] 2000/520/EG: Kommissionens beslut av den 26 juli 2000 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom de principer om integritetsskydd (Safe Harbor Privacy Principles) i kombination med frågor och svar som Förenta staternas handelsministerium utfärdat

[28] Magnusson Sjöberg, personuppgiftslagen (1998:204), 33 §, Lexino den 2 juli 2017.

[29] EU-domstolens avgörande den 6 oktober 2015 i mål C-362/14, p. 79–98 och 99–106.

[30] Kommissionens genomförandebeslut (EU) 2016/1250 av den 12 juli 2016 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom skölden för skydd av privatlivet i EU och Förenta staterna

i stadgan för de registrerade. Detta kom till uttryck i domen genom att domstolen bl.a. konstaterade att övervakningsprogrammen var alltför vida och obegränsade sett till sin utformning. De registrerade hade inte några lagstadgade rättigheter i förhållande till de amerikanska myndigheter och vissa delar av övervakningsprogrammen grundade sig på beslut som inte var föremål för domstolskontroll.

Ytterligare en grund för domstolens bedömning var att avsaknaden av lagstadgade rättigheter innebar att de registrerade inte kunde vända sig till domstol för att begära en rättslig prövning av en rättighetsinskränkning. Visserligen innehöll Privacy Shield som nämnts en ombudsmannamekanism, men EU-domstolen ansåg att ett sådant institut inte var likvärdig en opartisk domstol bl.a. mot bakgrund av att ombudsmannen var en del av det amerikanska utrikesdepartementet.[31] Därigenom var inte beslutet om Privacy Shield förenligt med artikel 45.1 i dataskyddförordningen och ogiltigförklarades av EU-domstolen. [32]

EU-domstolens bedömning av de amerikanska övervakningsprogrammen får även bäring på andra metoder för överföring än just mekanismen i artikel 45.1. Domstolen konstaterade nämligen att bedömningen av skyddsnivå måste säkerställas oberoende av vilken bestämmelse i dataskyddsförordningen som ligger till grund för en överföring av personuppgifter till ett tredjeland.[33]

5.2 Kronofogdens överväganden kring adekvat skyddsnivå i anledning av EU-domstolens avgörande om Privacy Shield

Kronofogdens bedömning: Kronofogden får inte överföra personuppgifter till USA med stöd av EU-kommissionens beslut om Privacy Shield enligt artikel 45.1 i EU:s dataskyddsförordning.

Personuppgiftsöverföring till USA måste vila på andra rättsliga grunder.

Skäl för bedömningen: Kommissionens beslut om Privacy Shield upphävdes den 16 juli 2020 vilket innebär att överföring av personuppgifter till USA inte längre kan stödja sig på detta beslut. EU-domstolen uttrycker tydlig att det föreligger en omedelbar konflikt mellan utformningen av de amerikanska övervakningsprogrammen och EU:s rättighetsstadga.

I praktiken innebär domstolens avgörande stora begränsningar i möjligheterna att överföra personuppgifter till USA, även när överföringen sker med andra rättsliga grunder än Privacy Shield. Domen bör dock inte tolkas som ett absolut hinder för

[31] Se punkterna 180, 183 och 197 i C-311/18 - Facebook Ireland och Schrems.
[32] Se punkterna 199–200 i C-311/18 - Facebook Ireland och Schrems samt domslut under punkt 5.
[33] Se punkt 92 i C-311/18 - Facebook Ireland och Schrems

all personuppgiftsöverföring till USA. Det finns skäl att påminna sig om att problematiken med extraterritoriell tillämpning av utländsk lagstiftning inom unionens område var något som var känt redan vid dataskyddsförordningens tillkomst. Som framgår av skäl 115 innehåller unionsrätten överväganden kring vilka situationer som personuppgifter får överföras till tredjeland trots att överföringen innebär ett sämre skydd för de registrerade. Till detta kommer också att det finns andra skyddsmekanismer i regelverket för att personuppgifter olovligen inte ska föras ut ur den europeiska unionen.

Följden av att EU-domstolen har upphävt Privacy Shield blir att Kronofogden får grunda överföring av personuppgifter till USA på andra regler i den hierarki av bestämmelser som gäller vid överföring av personuppgifter till tredjeland enligt dataskyddsförordningen.

6 Överföring av personuppgifter till tredjeland på grundval av lämpliga skyddsåtgärder

6.1 Överföringar som omfattas av lämpliga skyddsåtgärder

Enligt artikel 46 i dataskyddsförordningen kan personuppgifter överföras till tredjeland utan ett beslut från kommissionen om adekvat skyddsnivå om det istället har vidtagits lämpliga skyddsåtgärder.

Enligt artikel 46.2, punkterna a–f, kan skyddsåtgärderna ta formen av

a) ett rättsligt bindande och verkställbart instrument mellan offentliga myndigheter eller organ,
b) bindande företagsbestämmelser i enlighet med artikel 47,
c) standardiserade dataskyddsbestämmelser som antas av kommissionen i enlighet med det granskningsförfarande som avses i artikel 93.2,
d) standardiserade dataskyddsbestämmelser som antagits av en tillsynsmyndighet och godkänts av kommissionen i enlighet med det granskningsförfarande som avses i artikel 93.2,
e) en godkänd uppförandekod enlig artikel 40 tillsammans med rättsligt bindande och verkställbara åtaganden för den personuppgiftsansvarige eller personuppgiftsbiträdet i tredjelandet att tillämpa lämpliga skyddsåtgärder, även när det gäller registrerades rättigheter, eller
f) en godkänd certifieringsmekanism enlig artikel 42 tillsammans med rättsligt bindande och verkställbara åtaganden för den personuppgiftsansvarige, personuppgiftsbiträdet i tredjelandet att tillämpa lämpliga skyddsåtgärder, även när det gäller de registrerades rättigheter.

Punkt a syftar till internationella avtal mellan en eller flera myndigheter inom EU och en eller flera myndigheter utanför unionen och punkt b handlar om överföring

av personuppgifter inom en internationell koncern. Punkt c och d handlar om standardiserade dataskyddsbestämmelser, dvs. avtalsklausuler, som antagits av kommissionen eller av en tillsynsmyndighet med kommissionens godkännande. Dataskyddsklausulerna är formulerade som bindande villkor för avtalsparterna med skyldigheter kring information, rätt för tredje part (dvs. de registrerade) att åberopa villkoren, skadestånd, förbud kring ändring av villkor m.m.[34] Syftet är att avtalsrättsligt reglera dataskyddet för de registrerade. Punkt e och f handlar om att skapa skyddsåtgärder genom uppförandekoder eller certifieringar, typiskt sett branschspecifika dataskyddsregler som tas fram av branschorganisationer enligt artikel 40–42 i dataskyddsförordningen. I denna kontext måste uppförandekoder eller certifieringsmekanismerna eller uppförandekoderna också vara rättsligt bindande och verkställbara för mottagaren av uppgifterna i tredjeland.[35]

6.2 Särskilt om standardavtalsklausulerna enligt 46.2 c

Punkt c var föremål för EU-domstolens prövning i Schrems II, dvs. frågan om giltigheten av kommissionens beslut om standardavtalsklausulernas och dess tillämpning. I denna kontext handlar skyddsåtgärden som nämnts om att den personuppgiftsansvarige ingår ett avtal med mottagaren av informationen utanför unionen. Avtalet ska då innehålla de standardiserade dataskyddsbestämmelser som antagits av kommissionen. Tidigare kommissionsbeslut enligt 1995 års dataskyddsdirektiv är fortsatt giltiga enligt 46.5.

De gällande standardklausulerna är följande, varav den sista handlar om överföring av personuppgifter till personuppgiftsbiträden i länder utanför EU/EES.

- 2001/497/EG: Kommissionens beslut av den 15 juni 2001 om standardavtalsklausuler för överföring av personuppgifter till tredjeland enligt direktiv 95/46/EG
- 2004/915/EG: Kommissionens beslut av den 27 december 2004 om ändring av beslut 2001/497/EG om standardavtalsklausuler för överföring av personuppgifter till tredjeland
- 2010/87/: Kommissionens beslut av den 5 februari 2010 om standardavtalsklausuler för överföring av personuppgifter till registerförare etablerade i tredjeland i enlighet med Europaparlamentets och rådets direktiv 95/46/EG

Avtalen får enligt skäl 109 även behandla andra frågor under förutsättningen att övriga avtalsvillkor inte står i strid med standardavtalsklausulerna.

---

[34] Se exempelvis klausulerna i Kommissionens beslut av den 5 februari 2010 om standardavtalsklausuler för överföring av personuppgifter till registerförare etablerade i tredjeland i enlighet med Europaparlamentets och rådets direktiv 95/46/EG

[35] Europeiska dataskyddsstyrelsen har tagit fram riktlinjer för utformning om uppföranderegler och certifieringsmekanismer.

Kronofogden

Kronofogdemyndighetens ställningstagande

Beslutad av
Ulrika Lindén

Dokumentägare
Soheil Roshanbin

Gäller fr.o.m.
2021-02-04

Ansvarig organisation
Rättsavdelningen

Beslutsdatum
2021-02-04

Ny

Nr
1/21/RKF

Dnr
KFM 25972-2020

EU-domstolen konstaterade i Schrems II, p. 105, att artikel 46.1 och 46.2 c dataskyddsförordningen inte får tillämpas på ett sådant sätt de registrerades lagstadgade rättigheter och rätten till effektiva rättsmedel undergrävs. Den personuppgiftsansvarige kan därför inte enbart nöja sig med att konstatera att skyddsnivån som skapas genom att standardavtalsklausulerna tas in i ett avtal är tillräckligt god utan måste också bedöma hur uppgifterna kommer att hanteras enligt det mottagande landets rättssystem och den åtkomst som myndigheterna i det tredjelandet får åtkomst till.

Samtidigt uttalade domstolen (p.132–137) att det inte finns några hinder för den personuppgiftsansvarige att vidta kompensatoriska åtgärder i kombination med standardavtalsklausulerna, beroende på den situation som finns i det tredjelandet, för att säkerställa att skyddsnivån iakttas. Det är först när det inte finns en reell möjlighet att upprätthålla rättigheterna enligt artiklarna 7, 8 och 47 i stadgan som personuppgiftsöverföringen måste upphöra. Domstolen konstaterade i övrigt, (p. 138–148), att de befintliga standardavtalsklausulerna innehåller effektiva mekanismer som gör det möjligt att säkerställa att överföring av personuppgifter till tredjeland avbryts eller förbjuds om mottagaren inte iakttar eller inte kan iaktta klausulernas innehåll.

Sammantaget stod inte kommissionens beslut om standardavtalsklausuler enligt 46.2 c i strid med de grundläggande rättigheterna och därmed kan de användas som ett medel för överföring av personuppgifter till tredjeland under den förutsättningen att det skydd som erbjuds genom klausulerna är reella.

I kölvattnet av Schrems II har den Europeiska dataskyddstyrelsen tagit fram två stöddokument för att underlätta för den personuppgiftsansvariga att vidta lämpliga skyddsåtgärder vid överföring av uppgifter till tredjeland.

Den ena, ”Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data”, ger vägledning och metodstöd för tillämpning av artikel 46.2 c med bl.a. rekommendationer kring vad som ska bedömas och vilka förstärkande åtgärder som den personuppgiftsansvarige kan vidta för att nå upp till rätt skyddsnivå för de registrerade. Som exempel kan nämnas tekniska åtgärder såsom kryptering, pseudonymisering eller fragmentisering av uppgifterna för att förhindra olovlig åtkomst. Ytterligare rekommendationer som bör uppmärksammas är hur skyddsåtgärder kan utformas som avtalsenliga villkor för mottagaren kring öppenhet om hur informationen behandlas i mottagarens land och avtalsvillkor kring skyldighet för mottagaren att vidta rättsliga åtgärder för att förhindra eller begränsa att informationen överlämnas till det mottagande landets myndigheter m.m.

Det andra dokumentet, ”Recommendations 02/2020 on the European Essential Guarantees for surveillance measures” syftar till att ge vägledning kring vilka bedömningskriterier som den personuppgiftsansvarige ska utgå ifrån vid bedömning av om övervakningsprogram i tredjeland står i konflikt med dataskyddsregleringen och grundläggande rättigheter.

6.3 Kronofogdemyndighetens överväganden kring överföring med stöd av lämpliga skyddsåtgärder

Kronofogdens bedömning: Kronofogden kan för överföring av personuppgifter till tredjeland använda sig av de av EU-kommissionen fastställda standardavtalsklausulerna. Detta förutsätter särskilda överväganden där personuppgiftsskyddet vid överföring till USA behöver kompletteras av genom t.ex. kontraktuella, tekniska eller organisatoriska åtgärder.

Vid en sådan överföring ska de registrerade ha ett tillräckligt skydd för sina personuppgifter och även rätt till ett effektivt rättsmedel även när personuppgiftsbehandlingen i sig inte innebär ett intrång i privatlivet. Förhandssamråd bör i svårbedömda fall ske med Integritetsskyddsmyndigheten.

Skäl för bedömningen: Om Kronofogden har ett behov av överföring av personuppgifter till tredjeland där det som i fallet med USA inte finns ett beslut från kommissionen om att landet har adekvat skyddsnivå kvarstår möjligheten för Kronofogden att ingå ett eget dataskyddsavtal med mottagaren genom tillämpningen av standardavtalsklausulerna.

Mot bakgrund av vad som har redogjorts i föregående avsnitt är tröskeln för att kunna utforma lämpliga skyddsåtgärder så hög att det främst kan bli aktuellt att överföra uppgifter med stöd av standardavtalsklausuler i situationer när det är uppgifter som utifrån ett integritetsperspektiv framstår som okänsliga. En bedömning av uppgiftens karaktär är dock inte tillräcklig. Som framgår av EU-domstolens avgörande måste de registrerade åtnjuta ett tillräckligt skydd för sina personuppgifter och ha en rätt till ett effektivt rättsmedel även när personuppgiftsbehandlingen i sig inte innebär ett intrång i privatlivet. Det ligger i sakens natur att det bör finnas större utrymme för att kunna åstadkomma ett tillräckligt skydd för de registrerade genom lämpliga skyddsåtgärder när uppgifterna i sig inte är känsliga.

Enligt Europeiska dataskyddsstyrelsens rekommendationer om ytterligare åtgärder för hur ett tillräckligt skydd för personuppgifter kan upprätthållas behöver den personuppgiftsansvarige bedöma vad det är för typ av uppgifter som behandlas genom överföringen, vilka risker som är förknippade med överföring och vilka tekniska, avtalsenlig och organisatoriska förstärkningsåtgärder som kan vidtas för att nå upp till en tillräcklig skyddsnivå för de registrerade. En sådan bedömning måste också

göras från fall till fall och med utgångspunkt från vilken typ av information som överförs.

Med hänsyn till vad som framkommit om utformningen av de amerikanska övervakningsprogrammen är användning av standardavtalsklausuler förenat med svårigheter och risker. Det finns anledning att tro att Kronofogden vid ett övervägande om att använda sig standardavtalsklausuler inte sällan kommer att ha behov att begära förhandssamråd med Integritetskyddsmyndigheten

7 Överföring av personuppgifter till tredjeland med stöd av tillämpliga undantagsregler

7.1 Undantag i vissa särskilda situationer

Enligt artikel 49.1 får överföring av personuppgifter till tredjeland ske trots avsaknad av ett beslut om adekvat skyddsnivå enligt artikel 45.3 eller lämpliga skyddsåtgärder enligt artikel 46 men under följande villkor.

a) Den registrerade har uttryckligen samtyckt till att uppgifterna får överföras, efter att först ha blivit informerad om de eventuella riskerna med sådana överföringar för den registrerade när det inte föreligger något beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder.

b) Överföringen är nödvändig för att fullgöra ett avtal mellan den registrerade och den personuppgiftsansvarige eller för att genomföra åtgärder som föregår ett sådant avtal på den registrerades begäran.

c) Överföringen är nödvändig för att ingå eller fullgöra ett avtal mellan den personuppgiftsansvarige och en annan fysisk eller juridisk person i den registrerades intresse.

d) Överföringen är nödvändig av viktiga skäl som rör allmänintresset.

e) Överföringen är nödvändig för att kunna fastställa, göra gällande eller försvara rättsliga anspråk.

f) 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.

g) Överföringen görs från ett register som enligt unionsrätten eller medlemsstaternas nationella rätt är avsett att ge allmänheten information och som är tillgängligt antingen för allmänheten eller för var och en som kan styrka ett

berättigat intresse, men endast i den utsträckning som de i unionsrätten eller i medlemsstaternas nationella rätt angivna villkoren för tillgänglighet uppfylls i det enskilda fallet.

Enligt 49.1 andra punkten finns ytterligare en ventil för överföring när övriga undantag inte är tillämpliga. Bestämmelsen förutsätter en intresseavvägning och tar sikte på enstaka, nödvändiga överföringar för ett berättigat ändamål. De registrerade och tillsynsmyndigheten ska då underrättas om överföringen.

Samtycke och avtal, det vill säga punkterna a-c i punkt får inte omfatta åtgärder som vidtas av offentliga myndigheter som ett led i utövandet av deras offentliga befogenheter. När det gäller punkt d i första stycket framgår det av artikel 49 att det ska vara ett erkänt intresse i unionsrätten eller i den nationella rätten som den personuppgiftsansvarige omfattas av.

Europeiska dataskyddsstyrelsen har gett ut riktlinjer om tillämpningen av artikel 49.[36]

7.2 Särskilt om undantag med den registrerades samtycke

Som nämnts får en överföring av personuppgifter till ett tredjeland ske om den registrerade uttryckligen har samtyckt till att personuppgifterna får överföras enligt punkt a, dvs. att samtycket ska specifikt avse överföringen. En förutsättning är att den registrerade ska ha informerats om riskerna med överföringen när det inte finns något beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder.

Begreppet samtycke definieras i artikel 4.11 som varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne.

Vad som avses med *frivillig* utvecklas i dataskyddsförordningens skäl 43. Där anges bl.a. att samtycke inte bör utgöra en giltig rättslig grund i ett särskilt fall där det råder betydande ojämlikhet mellan den registrerade och den personuppgiftsansvarige, särskilt om den personuppgiftsansvarige är en offentlig myndighet och det därför är osannolikt att samtycket har lämnats frivilligt när det gäller alla förhållanden som denna särskilda situation omfattar.

I skäl 42 anges att samtycke inte bör betraktas som frivilligt om den registrerade inte har någon genuin eller fri valmöjlighet eller inte utan problem kan vägra eller

[36] Riktlinjer 2/2018 för undantagen i artikel 49 enligt förordning 2016/679.

ta tillbaka sitt samtycke. Av skäl 42 framgår också att ett *informerat* samtycket förutsätter att den registrerade ska känna till åtminstone den personuppgiftsansvariges identitet och syftet med den behandling för vilken personuppgifterna är avsedda.[37]

Hur ett samtycke bör lämnas för att den registrerade ska anses ha *godtagit behandlingen* behandlas i dataskyddsförordningens skäl 32. Samtycke bör lämnas genom en entydig bekräftande handling som innebär ett frivilligt, specifikt, informerat och otvetydigt medgivande från den registrerades sida om att denne godkänner behandling av personuppgifter rörande honom eller henne, som t.ex. genom en skriftlig, inklusive elektronisk, eller muntlig förklaring. Dataskyddsförordningens bestämmelser medger att ett samtycke lämnas genom faktiskt handlande.

Närmare villkor för samtycket anges i art. 7 dataskyddsförordningen. Där anges bl.a. att om behandlingen grundar sig på samtycke, ska den personuppgiftsansvarige kunna visa att den registrerade har samtyckt till behandling av sina personuppgifter (1 p.). Vidare anges att de registrerade ska ha rätt att när som helst återkalla sitt samtycke. Återkallandet av samtycket ska inte påverka lagligheten av behandling som grundar sig på samtycke, innan detta återkallas. Innan samtycke lämnas ska den registrerade informeras om detta. Det ska vara lika lätt att återkalla som att ge sitt samtycke (3 p.).

Europeiska dataskyddsstyrelsen har gett ut riktlinjer om samtycke enligt dataskyddsförordningen.[38] I riktlinjerna tas särskilt upp problematiken kring samtycke inom anställning bl.a. mot bakgrund av den maktobalans som finns mellan arbetsgivare och arbetstagare. Enligt riktlinjerna är det emellertid inte uteslutet med samtycke som en laglig grund för behandling av personuppgifter men det är endast tillåtet under förutsättning att inga negativa konsekvenser kommer att uppstå oavsett om den anställde ger sitt samtycke eller inte.[39]

7.3 Särskilt om viktiga skäl som rör allmänintresse

Enligt punkt 49.1 d får en överföring av personuppgifter till ett tredjeland ske om överföringen är nödvändig av viktiga skäl som rör allmänintresset. Av 49.4 framgår att allmänintresset ska vara erkänt i unionsrätten eller i den nationella rätten.

Vad begreppet allmänt intresse betyder kan härledas till skäl 112. Där anges som exempel internationella utbyten av uppgifter mellan konkurrensmyndigheter,

[37] I artikel 13 finns ytterligare krav på information som ska lämnas till den registrerade när uppgifterna samlas in från denne
[38] Guidelines 05/2020 on consent under Regulation 2016/679, antagna den 4 maj 2020.
[39] Ibid. s. 9.

skatte- eller tullmyndigheter, finanstillsynsmyndigheter, socialförsäkringsmyndigheter eller hälsovårdsmyndigheter, till exempel vid kontaktspårning för smittsamma sjukdomar eller för att minska och/eller undanröja dopning inom idrott. Begreppet allmänt intresse enligt artikel 49.1 är densamma som artikel 6.1.e och ska ha stöd i nationella författningar enligt artikel 6.3.[40]

En viktig aspekt av tillämpningen av artikel 49 är nödvändighetsprövningen, dvs. att det måste finnas ett verkligt skäl till varför uppgifterna behöver överföras och hur det förhåller sig till ändamålet. Ytterligare en aspekt som aktualiserats till följd av Schrems II handlar om hur frekvent eller återkommande undantagsreglerna enligt artikel 49 kan och får tillämpas. Av skäl 111 framgår att tillämpningen av artikel 49 vid samtycke, rättsliga anspråk m.m. och avtal ska vara tillåtna i fråga om tillfälliga överföringar medan motsvarande skrivningar inte finns för tillämpningen av artikel 49 för att lösa uppgifter av allmänt intresse.

Dataskyddstyrelsen tycks vara av uppfattning att även om en överföring på grund av ett allmänt intresse inte är begränsad till tillfälliga överföringar så betyder inte det att personuppgiftsöverföring får ske systematiskt och i stor omfattning med stöd av artikel 49. Undantagsreglerna i artikel 49 bör alltså inte användas som en huvudregel för överföring i den praktiska tillämpningen.[41]

För Kronofogden finns bestämmelser om myndighetens uppgifter i förordning (2016:1333) med instruktion för Kronofogdemyndigheten, men även i författningar som, ofta på detaljerad nivå, reglerar myndighetens uppgifter i olika avseenden, exempelvis utsökningsbalken (1981:774), lagen (1990:746) om betalningsföreläggande och handräckning, skuldsanerings (2016:675) och F-skuldsaneringslagen (2016:676) samt konkurslagen (1987:672) m.fl. Det finns även allmänna förvaltningsrättsliga regler i t.ex. tryckfrihetsförordningen, offentlighets- och sekretesslagen (2009:400) samt förvaltningslagen (2017:900). Uppgifter som utförs i anledning av dessa författningar omfattas som huvudregel av begreppet uppgift av allmänt intresse.

7.4 Kronofogdens överväganden kring överföring med stöd av tillämpliga undantagsregler

Kronofogdens bedömning: Om en överföring till tredjeland är nödvändig för att myndigheten ska kunna fullgöra en uppgift av allmänt intresse samtidigt som det saknas stöd för överföringen i artikel 46 (t.ex. standardavtalsklausulerna) får

[40] Se Öhman, Dataskyddsförordningen (GDPR) m.m. (29 februari 2020, Juno) kommentaren till artikel 49.

[41] Se fråga 8 i Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, publicerat den 24 juli 2020.

Kronofogden

Kronofogdemyndighetens ställningstagande

Beslutad av
Ulrika Lindén

Ansvarig organisation
Rättsavdelningen

Nr
1/21/RKF

Dokumentägare
Soheil Roshanbin

Beslutsdatum
2021-02-04

Dnr
KFM 25972-2020

Gäller fr.o.m.
2021-02-04

Ny

överföringen i enskilda fall göras med stöd av artikel 49 i dataskyddsförordningen.

Riskerna för de registrerades fri- och rättigheter måste vid en sådan överföring alltid prövas enligt dataskyddsförordningens säkerhetsbestämmelser.

Skäl för bedömningen: Om Kronofogden bedömer att det inte går att överföra personuppgifter till tredjeland med lämpliga skyddsåtgärder enligt artikel 46.2 c och det saknas andra alternativ för överföring kan myndigheten överväga att överföra personuppgifter med stöd av tillämpliga undantag i artikel 49. De situationer som blir aktuella i detta sammanhang är när det är nödvändigt för att lösa ett viktigt allmänintresse. I vissa situationer kan det vara aktuellt att uppgiften överförs till tredjeland efter samtycke från de registrerade.

En grundläggande förutsättning för tillämpning av undantagsbestämmelsen är att det är nödvändigt att just överföra personuppgifterna för viktiga skäl som rör allmänintresset. I många situationer kan en uppgift t.ex. lösas utan överföring av personuppgifter med enklare förändringar av arbetssätt. För att illustrera detta ges följande exempel. En myndighet vill publicera allmän information genom spridning på sociala medier. Om myndighetens medarbetare loggar in på plattformen med privata inloggningsuppgifter skulle inloggningen innebära en personuppgiftsöverföring till tredjeland. Om myndighetens medarbetare istället kan logga in med inloggningsuppgifter som tillhör myndigheten eller med fiktiva uppgifter skulle inte några personuppgifter föras över till tredjeland.

Förutom situationer när själva informationsutbytet och innehållet behövs för att lösa en uppgift av allmänt intresse, exempelvis mellan myndigheter i tredjeland, uppstår även andra fall av personuppgiftsöverföring där tillämpningen av artikel 49.1 d blir aktuell. Ett konkret exempel på en sådan situation är när en medarbetare på Kronofogden letar efter utmätningsbara tillgångar i olika it-tjänster bl.a. sociala medier. I vissa situationer kan inte medarbetarens namn undgå att bli överförd i samband med utredningen. Överföringen av personuppgifter blir då en oönskad men nödvändig bieffekt av arbetsuppgiften som får överföras med stöd av artikel 49.1 d. I enlighet med den Europeiska dataskyddstyrelsens rekommendationer förutsätter tillämpningen av regeln först att andra mer lämpligare sätt att försöka lösa uppgiften på har uttömts.

Det går inte att utesluta att det också kan finnas eller uppkomma situationer där endast en möjlig digital tjänst finns att tillgå för att uppfylla ett viktigt samhällsintresse. I sådana situationer bör undantagsreglerna kunna bli tillämpliga i avvaktan på att Kronofogden finner alternativa lösningar som inte förutsätter undantagslösningar.

Kronofogden

Kronofogdemyndighetens ställningstagande

Beslutad av	Ansvarig organisation	Nr
Ulrika Lindén	Rättsavdelningen	1/21/RKF
Dokumentägare	Beslutsdatum	Dnr
Soheil Roshanbin	2021-02-04	KFM 25972-2020
Gäller fr.o.m.	Ny	
2021-02-04		

Ett annat exempel på en situation där en personuppgiftsöverföring till tredjeland kan bli aktuell med tillämpning av undantagsreglerna är Kronofogdens arbete med att motverka överskuldsättning. I sådana sammanhang handlar det då inte om regelbundna eller storskaliga personuppgiftsöverföringar utan typiskt sett att namn och bild på medverkande i filmer, reportage eller informationskampanjer publiceras på sociala medier där uppgifterna förs till tredjeland. Den undantagsgrund som kan bli aktuell i sådana situationer är artikel 49.1 d (allmänt intresse) i förening med artikel 49.1 a (samtycke). Det handlar då om en författningsreglerad uppgift som inte är led i Kronofogdens myndighetsutövning. Som beskrivs i avsnitt 7.2 krävs att det är ett informerat och reellt samtycke inte bara till själva uppgiftsbehandlingen utan också till överföring av personuppgifter till tredjeland.

Det kan vara svårt att inom ramen för arbetsgivarförhållande låta personal utföra arbetsuppgifter där de förväntas lämna sitt samtycke för bl.a. överföring av uppgifter till tredjeland. Typiskt sett ska detta inte ske på grund av den ojämnbördiga relationen mellan arbetsgivare och arbetstagare. Om Kronofogden såväl objektivt för en utomstående betraktare som subjektivt för de egna medarbetarna skapar förutsättningar för ett samtycke enligt artikel 49.1 a kan det undantagsvis vara en möjlighet som kan övervägas. Det får dock inte ingå som ett nödvändigt moment för medarbetarens förmåga att lösa sina arbetsuppgifter. De exempel som närmast kommer på tal handlar om bild och namnuppgifter i sociala medier i samband med externa evenemang som myndigheten anordnar.

Som nämnts tidigare i avsnitt 4.2 innebär inte tillämpningen av reglerna i artikel 49 något undantag från dataskyddsförordningens övriga dataskyddsregelverk. En överföring av personuppgifter med tillämpningen av artikel 49 förutsätter därför också en prövning enligt dataskyddsförordningens säkerhetsbestämmelser. Riskerna för de registrerades fri- och rättigheter måste vid en överföring till tredjeland alltid prövas enligt dataskyddsförordningens säkerhetsbestämmelser.

_____

Soheil Roshanbin