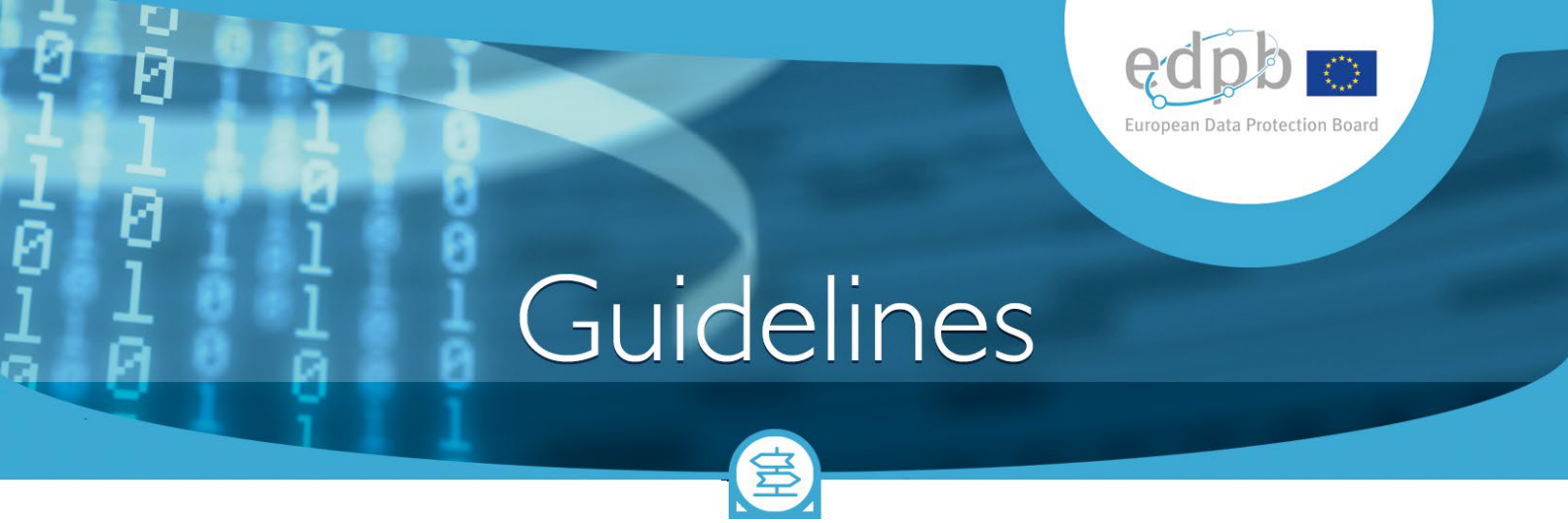


Riktlinjer 07/2022 om certifiering som överföringsverktyg

Version 2.0

Antagna den 14 februari 2023

Translations proofread by EDPB Members.
This language version has not yet been proofread.

VERSIONSHISTORIK

Version 1.0	av den 14 juni 2022	Antagande av riktlinjerna inför offentligt samråd
Version 2.0	av den 14 februari 2023	Antagande av riktlinjerna efter offentligt samråd

SAMMANFATTNING

Enligt artikel 46 i den allmänna dataskyddsförordningen ska en uppgiftsutförare vidta lämpliga skyddsåtgärder för överföring av personuppgifter till ett tredjeland eller internationella organisationer. För detta ändamål beskrivs i den allmänna dataskyddsförordningen de olika lämpliga skyddsåtgärder som uppgiftsutförare i enlighet med artikel 46 kan använda som ram för överföringar till tredjeland, bland annat genom att införa certifiering som en ny överföringsmekanism (artiklarna 42.2 och 46.2 f i dataskyddsförordningen).

Dessa riktlinjer ger vägledning om tillämpningen av artikel 46.2 f i den allmänna dataskyddsförordningen om överföring av personuppgifter till tredjeland eller till internationella organisationer på grundval av certifiering. Dokumentet är indelat i fyra avsnitt med en bilaga.

I del ett av detta dokument (”ALLMÄNT”) klargörs att riktlinjerna kompletterar de redan befintliga allmänna riktlinjerna 1/2018 om certifiering och att de tar upp särskilda krav i kapitel V i den allmänna dataskyddsförordningen när certifiering används som överföringsverktyg. Enligt artikel 44 i den allmänna dataskyddsförordningen måste varje överföring av personuppgifter till tredjeland eller internationella organisationer uppfylla villkoren i de övriga bestämmelserna i dataskyddsförordningen, utöver att efterleva kapitel V i dataskyddsförordningen. I ett första steg måste därför efterlevnaden av de allmänna bestämmelserna i den allmänna dataskyddsförordningen säkerställas, och i ett andra steg måste bestämmelserna i kapitel V i dataskyddsförordningen följas. De aktörer som medverkar och deras centrala roller i detta sammanhang beskrivs, med särskilt fokus på rollen för den uppgiftsinförare som kommer att beviljas en certifiering, och den uppgiftsutförare som kommer att använda den som ett ramverktyg för sina överföringar (med tanke på att ansvaret för databehandlingens lagenlighet ligger kvar hos uppgiftsutföraren). Certifieringen kan i detta sammanhang också omfatta åtgärder som kompletterar överföringsverktygen för att säkerställa överensstämmelse med EU:s skyddsnivå för personuppgifter. Del ett av riktlinjerna innehåller också information om processen för att erhålla en certifiering som ska användas som överföringsverktyg.

I den andra delen av dessa riktlinjer (”TILLÄMPNINGSRIKTLINJER FÖR ACKREDITERINGSKRAVEN”) erinras om att kraven för ackreditering av ett certifieringsorgan finns i ISO 17065 och att riktlinjerna 4/2018 om ackreditering av certifieringsorgan enligt artikel 43 i den allmänna dataskyddsförordningen och dess bilaga ska tolkas mot bakgrund av kapitel V. I samband med en överföring förklaras dock vissa av de ackrediteringskrav som gäller för certifieringsorganet ytterligare i dessa riktlinjer.

I den tredje delen av dessa riktlinjer (”SPECIFIKA CERTIFIERINGSKRITERIER”) ges vägledning om de certifieringskriterier som redan anges i riktlinjerna 1/2018 och fastställs ytterligare specifika kriterier som bör ingå i en certifieringsmekanism som ska användas som verktyg för överföring till tredjeland. Dessa kriterier omfattar bedömning av tredjelandets lagstiftning, uppgiftsutförares och uppgiftsinförares allmänna skyldigheter, regler om vidare överföring, prövning och verkställighet, förfaranden och åtgärder i situationer där nationell lagstiftning och praxis hindrar efterlevnad av åtaganden som gjorts inom ramen för certifiering och begäranden om tillgång till uppgifter från myndigheter i tredjeland.

Del fyra i dessa riktlinjer (”BINDANDE OCH VERKSTÄLLBARA ÅTAGANDEN SOM SKA GENOMFÖRAS”) innehåller inslag som bör tas upp i de bindande och verkställbara åtaganden som personuppgiftsansvariga eller personuppgiftsbiträden som inte omfattas av den allmänna dataskyddsförordningen bör göra i syfte att tillhandahålla lämpliga skyddsåtgärder för uppgifter som överförs till tredjeland. Dessa åtaganden, som kan anges i olika instrument, bl.a. avtal, ska särskilt omfatta en garanti för att uppgiftsinföraren inte har någon anledning att tro att den lagstiftning och praxis i tredjelandet som är

tillämplig på behandlingen i fråga, däribland eventuella krav på att lämna ut personuppgifter eller åtgärder som tillåter tillgång för offentliga myndigheter, hindrar uppgiftsinföraren från att fullgöra sina åtaganden enligt certifieringen.

BILAGAN till dessa riktlinjer innehåller några exempel på kompletterande åtgärder i linje med dem som förtecknas i rekommendationerna 01/2020 i bilaga II (Rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelsen med EU-nivån för skydd av personuppgifter) i samband med användningen av en certifiering som verktyg för överföring. Exemplen är utformade för att rikta uppmärksamheten mot kritiska situationer.

INNEHÅLLSFÖRTECKNING

Europeiska dataskyddsstyrelsen har antagit följande riktlinjer

med beaktande av artikel 70.1 e i 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 (nedan kallad *den allmänna dataskyddsförordningen*),

med beaktande av EES-avtalet, särskilt bilaga XI och protokoll 37, ändrat genom gemensamma EES-kommitténs beslut nr 154/2018 av den 6 juli 2018[1],

med beaktande av artiklarna 12 och 22 i dess arbetsordningen.

HÄRIGENOM FÖRESKRIVS FÖLJANDE

1 ALLMÄNT

1.1 Syfte och tillämpningsområde

1. Syftet med detta dokument är att ge vägledning om tillämpningen av artikel 46.2 f i den allmänna dataskyddsförordningen om överföring av personuppgifter till tredjeland eller till internationella organisationer på grundval av certifiering. Europeiska dataskyddsstyrelsen (EDPB) har redan offentliggjort allmänna riktlinjer om certifiering[2] och ackreditering[3] inom ramen för den allmänna dataskyddsförordningen. Dessa nya riktlinjer återspeglar därför endast de specifika aspekterna vad gäller certifiering som verktyg för överföringar. De specificerar tillämpningen av artiklarna 46.2 f och 42.2 i den allmänna dataskyddsförordningen genom att ge praktisk vägledning i detta avseende och införa nya inslag i de redan offentliggjorda riktlinjerna.

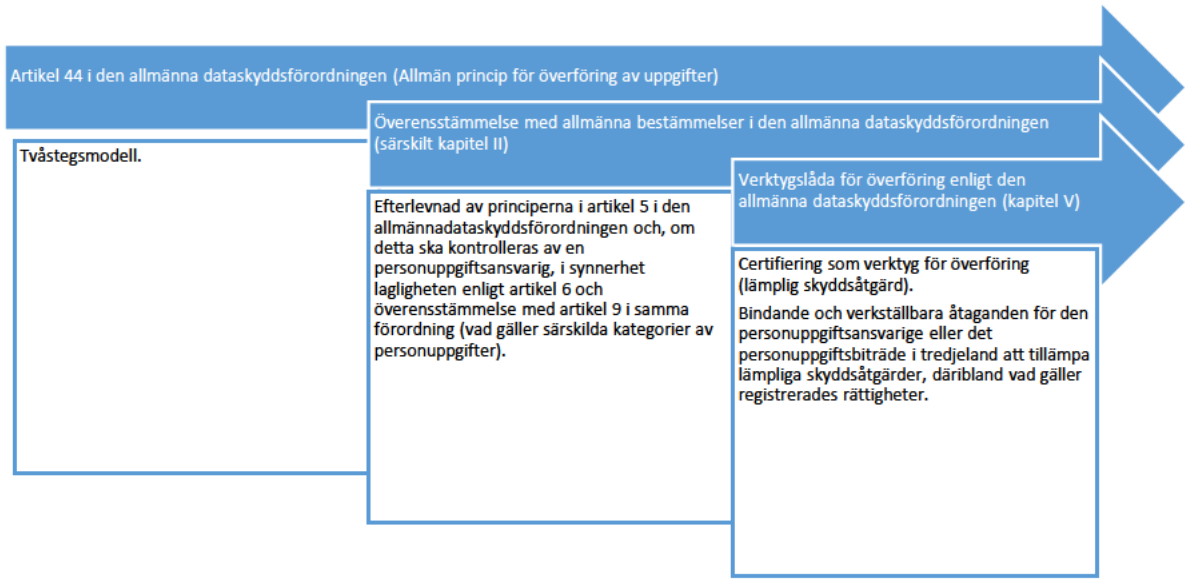
2. EDPB kommer att utvärdera hur dessa riktlinjer fungerar mot bakgrund av erfarenheterna av deras tillämpning i praktiken och ge ytterligare vägledning för att klargöra tillämpningen av de delar som förtecknas nedan, bl.a. certifieringsavtalets roll med avseende på de bindande och verkställbara åtaganden som avses i artikel 46.2 f i den allmänna dataskyddsförordningen.

1.2 Allmänna regler för internationella överföringar

3. Enligt artikel 44 i den allmänna dataskyddsförordningen måste varje överföring av personuppgifter till tredjeland[4] eller internationella organisationer uppfylla villkoren i de övriga bestämmelserna i dataskyddsförordningen, utöver att följa kapitel V i dataskyddsförordningen. Därför ska varje överföring vara förenlig med bland annat dataskyddsprinciperna i artikel 5 i allmänna dataskyddsförordningen, vara laglig enligt artikel 6 och överensstämma med artikel 9 i samma förordning om behandling av särskilda kategorier av personuppgifter. Därför ska ett tvåstegstest genomföras: Som ett första steg

[1]Hänvisningar till *medlemsstater* i detta dokument bör förstås som hänvisningar till *medlemsstater i EES*.
[2] Riktlinjer 1/2018 om certifiering och fastställande av certifieringskriterier i enlighet med artiklarna 42 och 43 i förordning 2016/679.
[3] Riktlinjer 4/2018 om ackreditering av certifieringsorgan enligt artikel 43 i allmänna dataskyddsförordningen (2016/679)
[4] Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR (inte översatt till svenska), sidan 4.

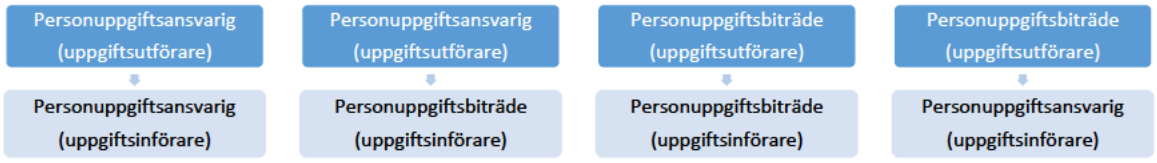
måste efterlevnaden av de allmänna bestämmelserna i den allmänna dataskyddsförordningen säkerställas, och som ett andra steg måste bestämmelserna i kapitel V i samma förordning följas.



4. I artikel 46 i allmänna dataskyddsförordningen anges att ”i avsaknad av ett beslut i enlighet med artikel 45.3, får en personuppgiftsansvarig eller ett personuppgiftsbiträde endast överföra personuppgifter till ett tredjeland eller en internationell organisation efter att ha vidtagit lämpliga skyddsåtgärder, och på villkor att lagstadgade rättigheter för registrerade och effektiva rättsmedel för registrerade finns tillgängliga”. Enligt artikel 46.2 f i den allmänna dataskyddsförordningen får sådana lämpliga skyddsåtgärder tillhandahållas genom en godkänd certifieringsmekanism tillsammans med bindande och verkställbara åtaganden för den personuppgiftsansvarige eller personuppgiftsbiträdet i tredjelandet att tillämpa lämpliga skyddsåtgärder, även vad gäller de registrerades rättigheter.

5. Till följd av detta kan uppgiftsutföraren besluta att förlita sig på den certifiering som en uppgiftsinförare erhållit för att visa att denne fullgör sina skyldigheter, t.ex. enligt artikel 24.3 eller artikel 28.5 i den allmänna dataskyddsförordningen. Uppgiftsinföraren kan besluta att ansöka om certifiering för att visa att det finns lämpliga skyddsåtgärder på plats.

6. Både uppgiftsutföraren och uppgiftsinföraren kan fullgöra olika roller (t.ex. som personuppgiftsansvarig eller personuppgiftsbiträde)[5], beroende på behandlingen i kapitel V, vilket leder till olika ansvarsområden:



7. Utöver användningen av certifiering eller något av de andra överföringsverktyg eller överföringsmekanismer som avses i artiklarna 45 och 46 föreskrivs i artikel 49 i den allmänna dataskyddsförordningen att internationella överföringar av uppgifter får ske i ett begränsat antal specifika situationer när ingen

[5] Se nedan: TILLÄMPNINGSRIKTLINJER FÖR ACKREDITERINGSKRAVEN.

annan mekanism i kapitel V efterlevs[6]. Enligt tidigare vägledning från EDPB måste dock de undantag som anges i artikel 49 i den allmänna dataskyddsförordningen tolkas restriktivt och främst gälla behandling av personuppgifter som är tillfällig och inte repetitiv[7].

1.3 Vilka är aktörerna och vilken roll spelar de för certifiering som verktyg för överföringar?

8. **Europeiska dataskyddsstyrelsen (EDPB)** har befogenhet att godkänna EES-omfattande certifieringskriterier (det europeiska sigillet för dataskydd) och avge yttranden om tillsynsmyndigheternas utkast till beslut om certifieringskriterier och ackrediteringskrav för certifieringsorganen för att säkerställa enhetlighet. Den är också behörig att sammanställa alla certifieringsmekanismer och sigill och märkningar för dataskydd i ett register och offentliggöra dem[8].

9. **Tillsynsmyndigheterna** godkänner certifieringskriterierna när certifieringsmekanismen inte är det europeiska sigillet för dataskydd[9]. De kan också ackreditera certifieringsorganet, utforma certifieringskriterierna och utfärda certifiering om detta fastställs i den nationella lagstiftningen i deras medlemsstat[10].

10. Det **nationella ackrediteringsorganet** får ackreditera tredjepartscertifieringsorgan genom att använda ISO 17065 och tillsynsmyndighetens ytterligare ackrediteringskrav, vilka bör vara i linje med avsnitt 2 i dessa riktlinjer. I vissa medlemsstater kan ackrediteringen även erbjudas av den behöriga tillsynsmyndigheten och utföras av ett nationellt ackrediteringsorgan eller av båda.

11. **Systemägare** är en organisation som har fastställt certifieringskriterierna och de metodkrav som ska uppfyllas vid bedömningen av överensstämmelse. Den organisation som gör bedömningarna kan vara samma organisation som har utvecklat och äger systemet, men det kan finnas arrangemang där en organisation äger systemet och en annan (eller flera andra) genomför bedömningarna som certifieringsorgan.

12. Beroende på nationell lagstiftning kan **certifieringsorganet**, som ackrediterats enligt ovan, utfärda certifieringarna istället för de behöriga tillsynsmyndigheterna[11]. Det kan utforma certifieringskriterier och därmed vara systemägare (se punkt 11 ovan). Det måste ha ett verksamhetsställe inom EES, särskilt för att möjliggöra ett effektivt utövande av de korrigerande befogenheter som fastställs i artikel 58.2 f i den allmänna dataskyddsförordningen. Certifieringsorganet kan dock lägga ut verksamhet på entreprenad till lokala experter eller inrättningar utanför EES som kommer att utföra revisionsverksamhet för dess räkning[12]. Ett certifieringsorgan får dock inte lägga ut beslutet om beviljande eller icke-beviljande av en certifiering på underentreprenad.

13. **Uppgiftsinföraren** är den enhet (personuppgiftsansvarig eller personuppgiftsbiträde) i tredjelandet som tar emot uppgifter från en uppgiftsutförare.

---

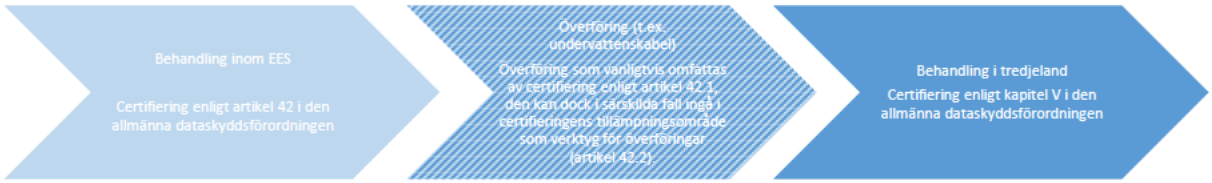
[6] För mer information om artikel 49 och sambandet med artikel 46 i allmänhet, se EDPB:s riktlinjer 2/2018 för undantagen i artikel 49 enligt förordning 2016/679.
[7] EDPB:s riktlinjer 2/2018 för undantagen i artikel 49 enligt förordning 2016/679, sida 5.
[8] Artikel 42.8 i den allmänna dataskyddsförordningen.
[9] Riktlinjer 1/2018 om certifiering och fastställande av certifieringskriterier i enlighet med artiklarna 42 och 43 i förordning 2016/679, punkt 2.2.
[10] Artiklarna 42.5 och 43.1 i den allmänna dataskyddsförordningen.
[11] Artikel 42.5 i den allmänna dataskyddsförordningen.
[12] Certifieringsorgan måste bedöma sina lokala experter i enlighet med ISO 17065 och de ytterligare ackrediteringskrav som fastställts av tillsynsmyndigheten (artikel 43.1 b i den allmänna dataskyddsförordningen).

14. **Uppgiftsutföraren** är den enhet (personuppgiftsansvarig eller personuppgiftsbiträde) som överför uppgifter från EES till en uppgiftsinförare. Uppgiftsutföraren måste se till att kapitel V följs.

1.4 Vad är tillämpningsområdet och objektet för certifieringen som verktyg för överföringar?

15. En certifieringsmekanism som ett överföringsverktyg enligt artikel 42.2 måste syfta till att säkerställa lämpliga skyddsåtgärder för behandling av personuppgifter enligt villkoren i artikel 46.2 f. Certifieringen ska visa att det finns lämpliga skyddsåtgärder som tillhandahålls av personuppgiftsansvariga eller personuppgiftsbiträden utanför EES eller som utgör en internationell organisation som tar emot uppgifter från personuppgiftsansvariga eller personuppgiftsbiträden inom EES för att motverka de specifika riskerna med att överföra personuppgifter.

16. I allmänhet utgör överföring av personuppgifter från en medlemsstat till ett tredjeland i sig behandling av personuppgifter i den mening som avses i artikel 4.2 i den allmänna dataskyddsförordningen, utförd i en medlemsstat[13] och som därför kan certifieras enligt artikel 42.1 i samma förordning. I vissa situationer kan dock, beroende på sammanhanget, även överföringen ingår i certifieringens tillämpningsområde som verktyg för överföringar. Följaktligen bör certifieringsobjektet – som sammanfaller med evalueringsobjektet under certifieringen[14] – i allmänhet vara behandlingen av de uppgifter som uppgiftsinföraren i tredjelandet mottagit från EES och överföringen, om den står under uppgiftsinförarens kontroll.



17. Certifieringsobjektet kan vara en enda behandling eller en serie åtgärder. Dessa kan omfatta styrningsprocesser i betydelsen organisatoriska åtgärder, vilket innebär att de utgör integrerade delar av en behandling[15].

18. Den enhet som ansöker skulle därför vara uppgiftsinföraren i tredjelandet med avseende på sitt certifieringsobjekt.

1.5 Vilken roll bör uppgiftsutförare spela i användningen av certifiering som överföringsverktyg?

19. Uppgiftsutförarens överföring omfattas som sådan i allmänhet direkt av den allmänna dataskyddsförordningen. Detta innebär att utföraren är skyldig att fullgöra sina skyldigheter enligt dataskyddsförordningen och i synnerhet att säkerställa att uppgifter överförs på ett säkert sätt i enlighet med artikel 32 och kapitel V för att säkerställa att den skyddsnivå för fysiska personer som garanteras genom den

---

[13] Europeiska unionens domstols dom i mål C-311/18 – Data Protection Commissioner/Facebook Ireland Ltd och Maximillian Schrems, nr 83.
[14] Riktlinjer 1/2018 om certifiering och fastställande av certifieringskriterier i enlighet med artiklarna 42 och 43 i förordning 2016/679, s. 17.
[15] Riktlinjer 1/2018 om certifiering och fastställande av certifieringskriterier i enlighet med artiklarna 42 och 43 i förordning 2016/679, s. 16 (t.ex. mekanismen för klagomålshantering)

förordningen inte undergrävs (artikel 44 i den allmänna dataskyddsförordningen)[16]. Detta kan naturligtvis certifieras enligt artikel 42.1.

20. Dessutom är uppgiftsutföraren som vill använda en certifiering som lämplig skyddsåtgärd enligt artikel 46.2 f i den allmänna dataskyddsförordningen särskilt skyldig att kontrollera om den certifiering som denne avser att förlita sig på är ändamålsenlig mot bakgrund av den avsedda behandlingens egenskaper. I detta syfte måste uppgiftsutföraren kontrollera den utfärdade certifieringen för att kontrollera om certifikatet är giltigt och inte har löpt ut, om den omfattar den specifika överföring som ska utföras och om överföringen av personuppgifter ingår i certifieringens tillämpningsområde, samt om det rör sig om vidare överföringar och om de åtföljs av tillräcklig dokumentation. Uppgiftsutföraren måste dessutom kontrollera att det certifieringsorgan som utfärdar certifieringen är ackrediterat av ett nationellt ackrediteringsorgan eller en behörig tillsynsmyndighet. Dessutom bör uppgiftsutföraren uppge användningen av certifieringen som verktyg för överföring i databehandlingsavtalet i enlighet med artikel 28 i den allmänna dataskyddsförordningen vid överföringar från personuppgiftsansvarig till personuppgiftsbiträde eller ett avtal om datadelning med uppgiftsinföraren i samband med överföringar mellan personuppgiftsansvariga.

21. Med tanke på att uppgiftsutföraren är ansvarig för att alla bestämmelser i kapitel V tillämpas måste uppgiftsutföraren också bedöma om den certifiering som uppgiftsutföraren avser att använda som ett verktyg för överföringar är ändamålsenlig mot bakgrund av gällande lagstiftning och praxis i tredjelandet som är relevanta för överföringen i fråga. För denna bedömning, och som en viktig faktor för att visa att uppgiftsutföraren uppfyller sitt ansvar, får uppgiftsutföraren förlita sig på den kontroll som utförs av certifieringsorganet av uppgiftsinförarens dokumenterade bedömning av tredjelandets lagstiftning och praxis.

22. Om uppgiftsinförarens bedömning har visat att denne och/eller uppgiftsutföraren kan behöva vidta kompletterande åtgärder i enlighet med certifieringen för att säkerställa en väsentligen likvärdig skyddsnivå som den som föreskrivs i EES, måste uppgiftsutföraren kontrollera de kompletterande åtgärder som tillhandahålls av den uppgiftsinförare som har en certifiering och om denne kan möta de tekniska och (i förekommande fall) kompletterande åtgärder som uppgiftsinföraren begär.

23. Om dessa krav inte uppfylls måste uppgiftsutföraren kräva att uppgiftsinföraren vidtar anpassade kompletterande åtgärder eller själv fastställer dem.

1.6 Hur ser processen ut för certifiering som ett verktyg för överföringar?

24. Certifieringen är frivillig, men när den söks måste den beviljas genom ett öppet förfarande som bygger på obligatoriska regler. Dataskyddsförordningen förlitar sig i hög grad på privata certifieringsmekan-

[16] I detta avseende är det viktigt att notera att det i artikel 44 i den allmänna dataskyddsförordningen tydligt anges att en överföring inte bara kan utföras av en personuppgiftsansvarig utan även av ett personuppgiftsbiträde. Det kommer därför att uppstå en överföringssituation när ett personuppgiftsbiträde skickar uppgifter till ett annat personuppgiftsbiträde eller till och med till en personuppgiftsansvarig i ett tredjeland i enlighet med den personuppgiftsansvariges instruktioner (artikel 28.3 a i den allmänna dataskyddsförordningen). I dessa fall agerar personuppgiftsbiträdet som uppgiftsutförare på den personuppgiftsansvariges vägnar och måste se till att bestämmelserna i kapitel V följs för den aktuella överföringen i enlighet med den personuppgiftsansvariges instruktioner, däribland att ett lämpligt överföringsverktyg används. Med tanke på att överföringen är en behandling som utförs på den personuppgiftsansvariges vägnar är den personuppgiftsansvarige också ansvarig och kan hållas till svars enligt kapitel V, och måste också se till att personuppgiftsbiträdet ger tillräckliga garantier enligt artikel 28.

ismer som en ”reglerad självreglering”. Följaktligen måste dessa mekanismer säkerställa att certifikaten väsentligen uppfyller kraven på lämpliga skyddsåtgärder enligt definitionen i artikel 46 i den allmänna dataskyddsförordningen.

25. Certifieringen måste därför baseras på en utvärdering av certifieringskriterierna enligt en bindande revisionsmetod. Dessa kriterier kommer att godkännas av nationella tillsynsmyndigheter eller av EDPB i enlighet med artikel 42.5 i den allmänna dataskyddsförordningen. Kriterierna för certifiering ska omfatta krav på en bedömning av uppgiftsinförarens behandling, bl.a. vidareöverföring, och av tredjelandets relevanta rättsliga ram, för att undvika att tredjelandets regler och praxis hindrar uppgiftsinföraren från att uppfylla sina skyldigheter enligt certifieringen.

26. Under certifieringsprocessen ska evalueringsobjektet kontrolleras enligt certifieringskriterierna av ett certifieringsorgan som ackrediterats av det nationella ackrediteringsorganet eller av den behöriga tillsynsmyndigheten[17].

27. Enligt artikel 43.1 i den allmänna dataskyddsförordningen ska certifieringsorgan som har lämplig nivå av expertis i fråga om dataskydd, efter att ha informerat tillsynsmyndigheten för att den ska kunna utöva sina befogenheter enligt artikel 58.2 h när så är nödvändigt, utfärda och förnya certifiering.

28. Enligt artikel 43.5 i den allmänna dataskyddsförordningen ska certifieringsorganen informera de behöriga tillsynsmyndigheterna om orsakerna till beviljandet eller återkallelsen av den begärda certifieringen. Detta innebär inte att certifieringsorganet behöver tillstånd från tillsynsmyndigheten för att utfärda certifiering. Certifieringsorganet avser att övervaka sina kunders efterlevnad av certifieringskriterierna.

29. Tillsynsorganet har korrigerande befogenhet att återkalla en certifiering eller beordra certifieringsorganet att återkalla en certifiering som utfärdats enligt artikel 42 eller 43 i den allmänna dataskyddsförordningen, eller anmoda certifieringsorganet att inte utfärda certifiering om kraven för certifiering inte längre uppfylls.

30. Ett europeiskt sigill för dataskydd för internationella överföringar av uppgifter kan fungera som ett verktyg för att täcka överföringar till tredjeland tillsammans med bindande och verkställbara åtaganden[18].

31. Certifieringar som ska användas som överföringsverktyg kan dock också utfärdas i enlighet med nationella godkända certifieringssystem i EES-staterna. De är därför endast giltiga för överföringar till tredjeland från uppgiftsutförare i den EES-medlemsstat där certifieringssystemet har godkänts, eftersom det inte finns något ömsesidigt erkännande av olika certifieringar i EES-staterna. Men tillsynsmyndigheter i olika EES-stater har rätt att godkänna samma certifieringsmekanism för överföringar[19].

---

[17] Riktlinjer 4/2018 om ackreditering av certifieringsorgan enligt artikel 43 i allmänna dataskyddsförordningen (2016/679), s. 9.

[18] Se artikel 42.5 i den allmänna dataskyddsförordningen och punkt 35 i EDPB:s riktlinjer 1/2018 om certifiering och fastställande av certifieringskriterier i enlighet med artiklarna 42 och 43 i förordningen.

[19] Om en tillsynsmyndighet leder antagandet av certifieringskriterierna X inom ramen för sitt nationella initiativ och andra länder därefter, med

beaktande av systemets kriterier och tillämpliga särskilda nationella bestämmelser, vill anta

samma certifieringskriterier, kan de anta dem utan att utlösa ett yttrande från Europeiska dataskyddsstyrelsen enligt artikel 64 i den allmänna dataskyddsförordningen och förlita sig på det yttrande som lämnats till den första

2 TILLÄMPNINGSRIKTLINJER FÖR ACKREDITERINGSKRAVEN

32. Kraven för ackreditering av ett certifieringsorgan med avseende på certifieringar som ett verktyg för överföringar återfinns i ISO 17065 och genom att riktlinjerna 4/201820 tolkas mot bakgrund av kapitel V, såsom förklaras nedan.

33. Enligt Europeiska dataskyddsstyrelsen omfattar de ytterligare ackrediteringskrav som utarbetats på grundval av riktlinjerna 4/2018 och ISO 17065 som antagits i enlighet med artikel 64.1 c i den allmänna dataskyddsförordningen redan de särskilda krav som krävs för ackreditering av ett certifieringsorgan vad gäller certifieringar som verktyg för överföringar. I ett överföringsscenario behöver dock vissa krav förbättras i fråga om förklarande anmärkningar och tolkning.

34. Vad gäller resurskraven (se krav 6 i riktlinjerna 4/2018 – bilaga 1) ska certifieringsorganet se till att det har de resurser som krävs för att kunna kontrollera att uppgiftsinföraren, i enlighet med certifieringskriterierna, på ett ändamålsenligt och korrekt sätt har gjort den nödvändiga bedömningen av rättslig situation och praxis i tredjeland, ett eller flera, där det är etablerat eller verksamt[21]. Denna bedömning bör göras med avseende på den behandling som ska certifieras som en del av evalueringsobjektet med avseende på lämpliga skyddsåtgärder enligt artikel 46 i den allmänna dataskyddsförordningen, och vid behov inbegripa de kompletterande åtgärder som identifierats och genomförts av uppgiftsinföraren. Detta inbegriper t.ex. betydande kunskaper om relevant lokal lagstiftning och praxis och lämpliga språkkunskaper i förhållande till tredjeland.

35. Vad gäller kraven med avseende på förfarandet (se krav 7 i bilaga 1 till riktlinjerna 4/2018) ska certifieringsorganet se till att certifieringsprocessen kan understödjas av eventuella revisioner på plats, att den utförs med avseende på den behandling som kommer att äga rum i tredjeland och att bedömningen även omfattar det praktiska genomförandet av befintlig lagstiftning och politik i tredjeland.

36. Vad gäller kraven på ändringar som påverkar certifieringen (se krav 7.10 i bilaga 1 till riktlinjerna 4/2018) ska certifieringsorganet övervaka ändringar av tredjelandets lagstiftning och/eller rättspraxis som kan påverka den behandling som omfattas av evalueringsobjektets tillämpningsområde.

3 SÄRSKILDA CERTIFIERINGSKRITERIER

37. I samband med beaktandet av de särskilda certifieringskriterierna bygger dessa riktlinjer på riktlinjerna 1/2018 om certifiering och identifiering av certifieringskriterier i enlighet med artiklarna 42 och 43 i förordningen (version 3. 0), motsvarande bilaga 2 om granskning och utvärdering av certifieringskriterier i enlighet med artikel 42.5 och tillägget till vägledningen om bedömning av certifieringskriterier.

38. De certifieringskriterier som utarbetats på grundval av riktlinjerna 1/2018 bilaga 2 och tillägget till vägledningen om bedömning av certifieringskriterier, omfattar redan, enligt EDPB, merparten av de certifieringskriterier som måste beaktas vid utarbetandet av ett certifieringssystem som ska användas som verktyg för överföringar. Det kan dock finnas ett behov av att ytterligare specificera vissa av dessa befintliga kriterier för att anpassa dem till ett specifikt överföringsscenario (se punkt 3.1). Dessutom

---

tillsynsmyndigheten, i enlighet med artikel 64.3 i samma förordning (se, i detta avseende, hänvisning till vägledning – addendum [bilaga till riktlinjer 1/2018 om certifiering och identifiering av certifieringskriterier i enlighet med artiklarna 42 och 43 i förordningen], punkt 66).

20 Riktlinjer 4/2018 om ackreditering av certifieringsorgan enligt artikel 43 i den allmänna dataskyddsförordningen och dess bilaga.

[21] Se punkt 12 ovan.

kan det finnas ett behov av att formulera ytterligare kriterier för tillämpningen av lämpliga skyddsåtgärder, även vad gäller de registrerades rättigheter (se punkt 3.2).

3.1 TILLÄMPNINGSRIKTLINJER FÖR CERTIFIERINGSKRITERIERNA

39. Vad gäller certifieringsmekanismens tillämpningsområde och evalueringsobjektet (se avsnitt 2 a i bilaga 2) bör detta beskrivas tydligt i relevant dokumentation, även vad gäller överföring av personuppgifter till tredjeland eller om avsikten är att även omfatta överföring av dem.

40. Vad gäller certifieringsmekanismens tillämpningsområde och evalueringsobjektet (se avsnitt 2 b i bilaga 2) bör relevant dokumentation innehålla en konkret beskrivning av vilken typ av enhet (t.ex. personuppgiftsansvarig och/eller personuppgiftsbiträde) som certifieringsmekanismen är tillämplig på.

41. Vad gäller certifieringsmekanismens tillämpningsområde och evalueringsobjektet (se avsnitt 2 f i bilaga 2) bör kriterierna kräva att utvärderingsmålen definieras på ett konkret sätt för att undvika missförstånd. I denna information bör åtminstone följande ingå:

42. Behandlingen/behandlingarna, även om vidare överföring planeras.

    a) Syftet.

    b) Typ av enhet (t.ex.: personuppgiftsansvarig och/eller personuppgiftsbiträde).

    c) Vilken typ av uppgifter som överförs, med beaktande av om det rör sig om särskilda kategorier av personuppgifter enligt definitionen i artikel 9 i dataskyddsförordningen.

    d) Kategorierna av de registrerade.

    e) De länder där databehandlingen äger rum.

43. Vad gäller insyn och de registrerades rättigheter (se bilaga 2, avsnitt 8) bör certifieringskriterierna

    a) kräva att information om behandlingen lämnas till registrerade, däribland i förekommande fall, information om överföring av personuppgifter till ett tredjeland eller en internationell organisation (se artiklarna 12, 13 och 14 i den allmänna dataskyddsförordningen),

    b) kräva att registrerade garanteras sin rätt till tillgång, rättelse, radering, begränsning, anmälan avseende rättelse eller radering av personuppgifter och begränsning av behandling, invändning mot behandling, rätt att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, bl.a. profilering, som i allt väsentligt är likvärdigt med de rättigheter som föreskrivs i artiklarna 15–19, 21 och 22 i den allmänna dataskyddsförordningen,

    c) kräva att ett lämpligt förfarande för hantering av klagomål inrättas av den uppgiftsinförare som innehar en certifiering för att säkerställa ett effektivt genomförande av den registrerades rättigheter,

    d) kräva en bedömning av huruvida och i vilken utsträckning dessa rättigheter är verkställbara för de registrerade i det berörda tredjelandet och eventuella ytterligare lämpliga åtgärder som kan behöva vidtas för att se till att de efterlevs, t.ex. krav på att uppgiftsinföraren kommer att gå med på att underkasta sig och samarbeta med den tillsynsmyndighet som är behörig för uppgiftsutföraren/uppgiftsutförarna i alla förfaranden som syftar till att säkerställa efterlevnaden av dessa rättigheter och, i synnerhet, att uppgiftsinföraren samtycker till att besvara förfrågningar, underkasta sig revisioner och följa de åtgärder som antagits av ovannämnda tillsynsmyndighet, bl.a. korrigerande och kompenserande åtgärder.

44. Vad gäller tekniska och organisatoriska åtgärder som garanterar skydd (avsnitt 10.q i bilaga 2) bör certifieringskriterierna kräva att uppgiftsinföraren informerar uppgiftsutföraren och, om uppgiftsinföraren agerar som personuppgiftsansvarig, underrättar den tillsynsmyndighet i EES som är behörig för uppgiftsutföraren eller uppgiftsutförarna om personuppgiftsbrott och informerar de registrerade om incidenten i de fall incidenten sannolikt kommer att medföra en hög risk för deras rättigheter och friheter, i enlighet med kraven i artikel 34 i den allmänna dataskyddsförordningen.

3.2 YTTERLIGARE SÄRSKILDA CERTIFIERINGSKRITERIER

45. Mot bakgrund av de skyddsåtgärder som fastställts för andra överföringsinstrument enligt artikel 46 i den allmänna dataskyddsförordningen (t.ex. bindande företagsregler eller uppförandekoder) och för att säkerställa en enhetlig skyddsnivå, och med beaktande av domstolens dom i Schrems II-målet, anser EDPB att certifieringsmekanismen som ska användas som verktyg för överföringar till tredjeland även bör omfatta de kriterier som anges nedan.

1. Bedömning av tredjelands lagstiftning

a) Krävs det enligt kriterierna att uppgiftsinföraren har bedömt regler och praxis i det tredjeland där denne är verksam och huruvida dessa hindrar uppgiftsinföraren från att uppfylla sina åtaganden enligt certifieringen?
b) Krävs det enligt kriterierna att uppgiftsinföraren dokumenterar bedömningen av regler och praxis i det tredjeland där denne är verksam och håller dokumentationen tillgänglig för certifieringsorganet och på begäran för den tillsynsmyndighet i EES som är behörig för uppgiftsutföraren och för uppgiftsutföraren?
c) Krävs det enligt kriterierna att uppgiftsinföraren har identifierat och genomfört de organisatoriska och tekniska åtgärderna för att tillhandahålla lämpliga skyddsåtgärder enligt artikel 46 i den allmänna dataskyddsförordningen, med beaktande av "Rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelsen med EU-nivån för skydd av personuppgifter"?
d) Krävs det enligt kriterierna att uppgiftsinföraren dokumenterar de organisatoriska och tekniska åtgärder som vidtagits på ett effektivt sätt för att tillhandahålla lämpliga skyddsåtgärder enligt artikel 46 i den allmänna dataskyddsförordningen och hålla dokumentationen tillgänglig för certifieringsorganet och på begäran för de behöriga dataskyddsmyndigheterna och uppgiftsutföraren?
e) Krävs det enligt kriterierna att uppgiftsinföraren har identifierat och genomfört organisatoriska och tekniska åtgärder för att säkerställa de överförda personuppgifternas säkerhet, med beaktande av rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelsen med EU-nivån för skydd av personuppgifter, om överföringen ingår i certifieringens tillämpningsområde som verktyg för överföringar?
f) Krävs det enligt kriterierna en garanti för certifieringsorganet och uppgiftsutföraren att uppgiftsinföraren inte har någon anledning att tro att den lagstiftning och praxis som är tillämplig på uppgiftsinföraren kan hindra denne från att uppfylla sina skyldigheter enligt certifieringen?

2. Allmänna skyldigheter för uppgiftsutförare och uppgiftsinförare

a) Krävs det enligt kriterierna att det i avtal (t.ex. i ett befintligt tjänsteavtal) mellan uppgiftsutförare och uppgiftsinförare fastställs en beskrivning av den specifika överföring som certifieringen gäller och att tredjepartsberättigade rättigheter erkänns för de berörda registrerade?

b) I den mån det enligt kriterierna krävs ett särskilt innehåll för dessa avtal eller instrument och en mall tillhandahålls, kräver kriterierna att de också är föremål för utvärderingen?

3. Regler för vidare överföring

a) Krävs det enligt kriterierna att vidare överföringar omfattas av särskilda skyddsåtgärder i enlighet med kraven i kapitel V i den allmänna dataskyddsförordningen för att säkerställa att den skyddsnivå som säkerställs inom EES inte undergrävs, och krävs det enligt kriterierna att lämplig dokumentation hålls tillgänglig för certifieringsorganet och den tillsynsmyndighet i EES som är behörig för uppgiftsutföraren/uppgiftsutförarna och uppgiftsutföraren på begäran?

4. Prövning och verkställighet

a) Föreskriver kriterierna att registrerade kan hävda sina rättigheter som tredjepartsberättigade gentemot uppgiftsinföraren vid EES-domstolen där den registrerade har sin hemvist, eller i en internationell organisation, bl.a. avseende ersättning för skada som den registrerade lidit om uppgiftsinföraren inte följer det relevanta certifieringssystemet?
b) Gör kriterierna det möjligt att på ett adekvat sätt bedöma om en uppgiftsinförare är ansvarig inom EES för den skada som den registrerade lidit vid bristande efterlevnad av det relevanta certifieringssystemet?
c) Krävs det enligt kriterierna att de registrerade kan lämna in ett klagomål mot uppgiftsinföraren till en tillsynsmyndighet i EES, särskilt i den EES-stat där han eller hon har sin vanliga vistelseort, sin arbetsplats eller är behörig för uppgiftsutföraren eller uppgiftsutförarna?
d) Krävs det enligt kriterierna att uppgiftsinföraren ska samarbeta med den tillsynsmyndighet i EES som är behörig för uppgiftsutföraren/uppgiftsutförarna och godta att bli föremål för revision och inspekteras av den (dem), ta hänsyn till dess (deras) råd och följa dess (deras) beslut?

5. Förfarande och åtgärder för situationer där den nationella lagstiftningen förhindrar efterlevnad av åtaganden som gjorts som en del av certifieringen

a) Krävs det enligt kriterierna ett åtagande om att om uppgiftsinföraren i ett tredjeland eller en internationell organisation har skäl att tro att ändringar i den lagstiftning och praxis som är tillämplig på denne kan hindra denne från att fullgöra sina skyldigheter enligt certifieringen, kommer denne omgående att anmäla detta till certifieringsorganet och uppgiftsutföraren, så att den senare kan bedöma om överföringen omedelbart ska stoppas?
b) Krävs det enligt kriterierna en beskrivning av de åtgärder som ska vidtas (inklusive anmälan till uppgiftsutföraren i EES och vidtagande av lämpliga ytterligare åtgärder) om uppgiftsinföraren får kännedom om lagstiftning eller praxis i ett tredjeland som förhindrar att skyldigheterna enligt certifieringen fullgörs, samt de åtgärder som ska vidtas vid

begäranden om information från myndigheter i tredjeland (däribland skyldigheten att granska och vid behov ifrågasätta ansökans lagenlighet och att minimera eventuell information som lämnas ut)?

6. Hantering av begäranden om åtkomst till uppgifter från myndigheter i tredjeland

a) Krävs det enligt kriterierna att uppgiftsinföraren omedelbart ska informera uppgiftsutföraren om myndigheter i tredjeland begär tillgång och vidta lämpliga ytterligare åtgärder?
b) Krävs det enligt kriterierna att överföringar till följd av oproportionerliga begäranden om tillgång från offentliga myndigheter i tredjeland, särskilt begäranden som kräver omfattande och godtyckliga överföringar av personuppgifter, inte ska äga rum?

7. Ytterligare skyddsåtgärder avseende uppgiftsutföraren

46. Krävs det enligt kriterierna att uppgiftsinföraren, när så planeras, även genom bindande krav på uppgiftsutföraren, säkerställer att de kompletterande åtgärder som denne har identifierat åtföljs av motsvarande kompletterande åtgärder från uppgiftsutförarens sida, med beaktande av EDPB:s rekommendationer 01/2020 och användningsfallen, för att säkerställa ett effektivt genomförande av uppgiftsinförarens kompletterande åtgärder?

4 BINDANDE OCH VERKSTÄLLBARA ÅTAGANDEN ATT GENOMFÖRA

47. Enligt 42.2 i den allmänna dataskyddsförordningen ska personuppgiftsansvariga och personuppgiftsbiträden som inte omfattas av dataskyddsförordningen och som iakttar en certifieringsmekanism avsedd för överföringar, dessutom göra bindande och verkställbara åtaganden, genom avtal eller andra rättsligt bindande instrument[22], att tillämpa de lämpliga skyddsåtgärder som föreskrivs enligt certifieringsmekanismen, bl.a. vad gäller registrerades rättigheter.

48. Som anges i den allmänna dataskyddsförordningen kan sådana åtaganden göras med ett avtal, vilket framstår som den enklaste lösningen. Även andra instrument kan användas, förutsatt att de personuppgiftsansvariga/personuppgiftsbiträden som iakttar certifieringsmekanismen kan uppvisa att dessa andra metoder är bindande och verkställbara till sin karaktär.

49. Under alla omständigheter måste den bindande och verkställbara karaktären säkerställas i EU-lagstiftningen, och åtagandena bör också vara bindande och verkställbara av registrerade i egenskap av tredjepartsmottagare.

50. Ett direkt alternativ skulle vara att inkludera bindande och verkställbara åtaganden i avtalet mellan uppgiftsutföraren och uppgiftsinföraren. I praktiken skulle parterna kunna använda ett befintligt avtal (t.ex. tjänsteavtal mellan uppgiftsutföraren och uppgiftsinföraren, avtalet om behandling av personuppgifter i enlighet med artikel 28 i den allmänna dataskyddsförordningen mellan personuppgiftsansvariga och personuppgiftsbiträden, eller ett avtal om datadelning mellan skilda personuppgiftsansvariga) i vilket de bindande och verkställbara åtagandena kan ingå. Dessa åtaganden bör tydligt särskiljas från alla andra klausuler. Ett annat alternativ skulle kunna vara att till exempel använda sig av ett se-

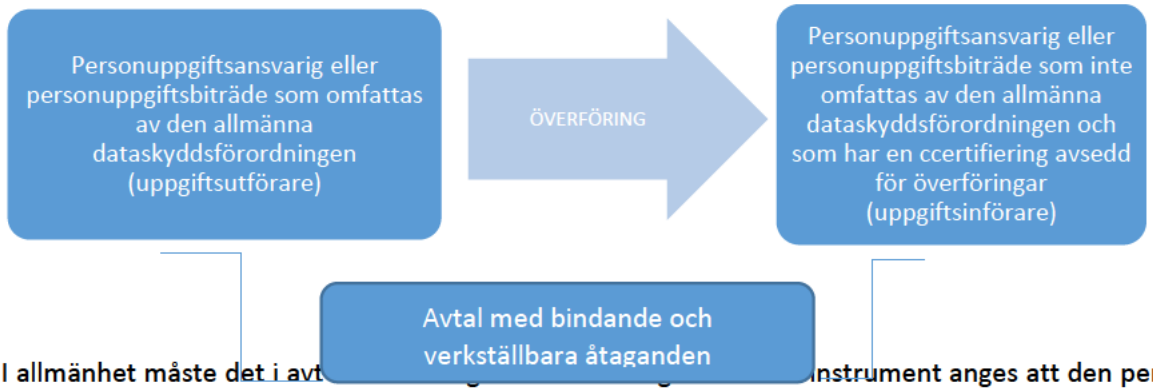
[22] Detta rättsligt bindande instrument ska inte vara något annat verktyg i kapitel V (t.ex. standardavtalsklausulen), eftersom de bindande och verkställbara åtaganden som avses i artikel 46.2 f måste utformas för att säkerställa att uppgiftsinföraren kommer att uppfylla certifieringskriterierna.

parat avtal genom att till den för överföringar avsedda certifieringsmekanismen lägga till ett modellavtal som sedan skulle behöva undertecknas av personuppgiftsansvariga/personuppgiftsbiträden i tredjeland och alla uppgiftsutförare.

51. Det bör finnas flexibilitet för att välja det lämpligaste alternativet beroende på den specifika situationen.

52. När certifieringsmekanismen ska användas för överföringar och vidareöverföringar från ett personuppgiftsbiträde till en underentreprenör, bör det i personuppgiftsbiträdesavtalet som ingås mellan personuppgiftsbiträdet och dennes personuppgiftsansvarige även göras en hänvisning till certifieringsmekanismen och det instrument som anger bindande och verkställbara åtaganden.

Exempel på bindande och verkställbara åtaganden som ingår i avtalet mellan uppgiftsutföraren och uppgiftsinföraren:



53. I allmänhet måste det i avt nstrument anges att den personuppgiftsansvarige eller det personuppgiftsbiträde som innehar ett certifikat och som agerar som uppgiftsinförare åtar sig att följa de regler som anges i den certifiering som är avsedd för överföringar när de relevanta uppgifterna från EES behandlas och garanterar att denne inte har någon anledning att tro att den lagstiftning och praxis i tredjelandet som är tillämplig på behandlingen i fråga, däribland eventuella krav på att lämna ut personuppgifter eller åtgärder som tillåter tillgång för offentliga myndigheter, hindrar denne från att fullgöra sina åtaganden enligt certifieringen och att denne kommer att informera uppgiftsutföraren om alla relevanta ändringar av lagstiftningen eller praxis i detta avseende.

54. I avtalet eller det andra instrumentet ska det också finnas mekanismer som gör det möjligt att verkställa sådana åtaganden i händelse av att den personuppgiftsansvarige/personuppgiftsbiträdet som agerar som uppgiftsinförare inte efterlever reglerna enligt certifieringen, i synnerhet med avseende på rättigheterna för registrerade vars uppgifter ska överföras enligt koden.

55. Närmare bestämt bör följande behandlas i avtalet eller det andra instrumentet:

- Förekomsten av en rättighet för registrerade vars uppgifter överförs inom ramen för certifieringen att som tredjepartsmottagare verkställa de åtaganden som gjorts av den certifierade uppgiftsinföraren inom ramen för certifieringen.

- Frågan om ansvar i händelse av att uppgiftsinföraren som har en certifiering utanför EES inte efterlever reglerna enligt certifieringen. De registrerade ska ha möjlighet att, i händelse av att en uppgiftsinförare som innehar en certifiering utanför EES inte efterlever reglerna enligt certifieringen, genom att åberopa sin rätt som berättigade tredjeparter ställa anspråk, däribland på ersättning, mot denna enhet vid en tillsynsmyndighet i EES och en domstol i EES där den registrerade har sin stadigvarande vistelseort. Uppgiftsinföraren som har en certifiering ska acceptera den registrerades beslut att göra detta. Registrerade ska också ha möjlighet att mot uppgiftsinföraren ställa anspråk, i händelse av bristande efterlevnad från uppgiftsinförarens sida

som skulle kunna leda till ansvarsskyldighet för uppgiftsutföraren, vid tillsynsmyndigheten eller domstolen för uppgiftsutförarens etableringsplats eller den registrerades stadigvarande vistelseort23. Uppgiftsinföraren och uppgiftsutföraren bör också godkänna att den registrerade kan företrädas av ett organ, organisation eller sammanslutning utan vinstsyfte enligt bestämmelserna i artikel 80.1 i den allmänna dataskyddsförordningen.

- Förekomsten av en rätt för uppgiftsutföraren att mot uppgiftsinföraren som innehar en certifiering verkställa reglerna enligt certifieringen som berättigade tredje part.
- Förekomsten av en skyldighet för uppgiftsinföraren som innehar en certifiering att underrätta uppgiftsutföraren och uppgiftsutförarens tillsynsmyndighet om alla åtgärder som vidtas av certifieringsorganet med anledning av en upptäckt bristande efterlevnad av certifieringsreglerna av samma uppgiftsinförare.

[23] Detta ansvar ska inte påverka de mekanismer som ska genomföras enligt certifieringen med certifieringsorganet som också kan vidta åtgärder mot certifierade personuppgiftsansvariga/personuppgiftsbiträden i enlighet med certifieringen genom att ålägga korrigerande åtgärder.

BILAGA

A. EXEMPEL PÅ KOMPLETTERANDE ÅTGÄRDER SOM SKA GENOMFÖRAS AV UPPGIFTSINFÖRAREN OM ÖVERFÖRINGEN INGÅR I CERTIFIERINGENS TILLÄMPNINGSOMRÅDE

Användningsfall 1: Datalagring för säkerhetskopiering och andra ändamål som inte kräver åtkomst till uppgifter i klartext

Kriterier för krypteringsstandarder och krypteringsnyckelns säkerhet, särskilt kriterier som rör den rättsliga situationen i tredjelandet, måste fastställas. Om uppgiftsinföraren kan tvingas överföra krypteringsnycklar kan den ytterligare åtgärden inte anses vara effektiv[24].

Användningsfall 2: Överföring av pseudonymiserade uppgifter

Vad gäller pseudonymiserade uppgifter ska kriterier fastställas för säkerheten hos de ytterligare uppgifter som krävs för att hänföra de överförda uppgifterna till en identifierad eller identifierbar person, särskilt följande:

- Kriterier avseende rättsläget i det tredje landet. Om uppgiftsinföraren kan tvingas att tillgå eller använda ytterligare uppgifter för att hänföra uppgifterna till en identifierad eller identifierbar person kan åtgärden inte anses vara effektiv[25].

- Kriterier som rör definitionen av ytterligare information som är tillgänglig för myndigheter i tredjeland och som kan vara tillräcklig för att uppgifterna ska kunna hänföras till en identifierad eller identifierbar person.

Användningsfall 3: Kryptering av uppgifter för att skydda dem från offentliga myndigheters åtkomst i uppgiftsinförarens tredjeland när de övergår mellan uppgiftsutföraren och dennes uppgiftsinförare

Vad gäller krypterade data ska alla kriterier för säkerheten vid överföringen inkluderas. Om uppgiftsinföraren kan tvingas vidarebefordra krypteringsnycklar för dekryptering eller autentisering eller ändra en komponent som används för överföring på ett sådant sätt att dess säkerhetsegenskaper undergrävs, kan den ytterligare åtgärden inte anses vara effektiv[26].

Användningsfall 4: Skyddad mottagare

Vad gäller skyddade mottagare måste kriterier för gränserna för sekretessen fastställas. Uppgiftsbehandlingen måste hållas inom gränserna för tystnadsplikt. Detta gäller även för behandling som utförs av (under)entreprenörer och vidare överföringar, vars mottagare också måste ha dessa privilegier[27].

---

[24] Bilaga 2, rekommendation 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelse med EU-nivån för skydd av personuppgifter, version 2.0, användningsfall 1: Datalagring för säkerhetskopiering och andra ändamål som inte kräver åtkomst till uppgifter i klartext, s. 85. https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_sv.pdf

[25] Se ovan, punkterna 86–89.

[26] Se ovan, punkt 90.

[27] Se ovan, punkt 91.

B. EXEMPEL PÅ KOMPLETTERANDE ÅTGÄRDER OM ÖVERFÖRINGEN INTE OMFATTAS AV CERTIFIERINGEN OCH UPPGIFTSUTFÖRAREN MÅSTE SE TILL ATT DE VIDTAS

Användningsfall 2: Överföring av pseudonymiserade uppgifter

Kriterier ska anges för den ytterligare information som myndigheterna i tredjelandet har tillgång till och som kan vara tillräcklig för att uppgifterna ska kunna hänföras till en identifierad eller identifierbar person.

Användningsfall 3: Kryptering av uppgifter för att skydda dem från offentliga myndigheters åtkomst i uppgiftsinförarens tredjeland när de övergår mellan uppgiftsutföraren och dennes uppgiftsinförare

Kriterier ska tillhandahållas avseende tillförlitligheten hos den certifikatutfärdare eller den infrastruktur som används, säkerheten hos de krypteringsnycklar som används för autentisering eller dekryptering och nyckelhanteringens tillförlitlighet samt användningen av korrekt underhållen programvara utan kända sårbarheter.

Om uppgiftsinföraren kan tvingas avslöja krypteringsnycklar som är lämpliga för dekryptering eller autentisering eller att ändra en komponent som används för överföring för att undergräva dess säkerhetsegenskaper, kan åtgärden inte anses vara effektiv[28].

Användningsfall 4: Skyddad mottagare

Vad gäller skyddade mottagare måste kriterier för gränserna för sekretessen fastställas. Uppgiftsbehandlingen måste hållas inom gränserna för tystnadsplikt. Detta gäller även för behandling som utförs av (under)entreprenörer och vidare överföringar, vars mottagare också måste omfattas av tystnadsplikt[29].

[28] Se ovan, rekommendationerna, punkt 90.
[29] Se ovan, rekommendationerna, punkt 91.