

Henstillinger



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

Henstilling nr. 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger

Version 2.0

Vedtaget den 18. juni 2021

Versionsoversigt

Version 2.0	18. juni 2021	Vedtagelse af henstillingen efter offentlig høring
Version 1.0	10. november 2020	Vedtagelse af henstillingen til offentlig høring

Resumé

EU's generelle databeskyttelsesforordning (GDPR) blev vedtaget for at opfylde to formål: at lette fri udveksling af personoplysninger inden for Den Europæiske Union og samtidig beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder, navnlig deres ret til beskyttelse af personoplysninger.

I sin dom for nylig C-311/18 (Schrems II) minder Den Europæiske Unions Domstol (EU-Domstolen) os om, at den beskyttelse, personoplysninger er sikret i Det Europæiske Økonomiske Samarbejdsområde (EØS), skal følge oplysningerne, uanset hvor de føres hen. Overførsel af personoplysninger til tredjelande må ikke være en metode til at underminere eller udvande den beskyttelse, der er sikret i EØS. Domstolen gentager dette ved at præcisere, at beskyttelsesniveauet i tredjelande ikke behøver at være identisk med det niveau, der er sikret i EØS, men det skal i det væsentlige være tilsvarende. Domstolen fastslår endvidere gyldigheden af standardbestemmelser om databeskyttelse som et overførselsværktøj, der kontraktligt kan sikre et beskyttelsesniveau, der i det væsentlige er tilsvarende, for data overført til tredjelande.

Standardbestemmelser om databeskyttelse og andre af de i artikel 46 i GDPR omtalte overførselsværktøjer fungerer ikke i et vakuum. Domstolen fastslår, at dataansvarlige eller databehandlere, der optræder som eksportører, er ansvarlige for i hvert enkelt tilfælde, og hvis det er relevant i samarbejde med importøren i tredjelandet, at undersøge, om lovgivningen eller praksis i tredjelandet kolliderer med effektiviteten af de fornødne garantier, der fremgår af overførselsværktøjer, jf. artikel 46 i GDPR. I disse tilfælde lader Domstolen det fortsat være op til eksportører at gennemføre supplerende foranstaltninger, der udfylder disse huller i beskyttelsen og sørge for, at de er på det niveau, der kræves i EU-retten. Domstolen specificerer ikke disse foranstaltninger. Domstolen understreger imidlertid, at eksportører i hvert enkelt tilfælde skal fastlægge dem. Dette er i overensstemmelse med ansvarlighedsprincippet i artikel 5, stk. 2, i GDPR, som pålægger dataansvarlige at være ansvarlige for og kunne påvise overholdelse af principperne i GDPR vedrørende behandling af personoplysninger.

Som hjælp til eksportører (uanset om det er dataansvarlige, databehandlere, private enheder eller offentlige organer, der behandler personoplysninger inden for rammerne af GDPR), med den komplekse opgave det er at vurdere tredjelande og om nødvendigt kortlægge passende supplerende foranstaltninger, har Det Europæiske Databeskyttelsesråd (Databeskyttelsesrådet) vedtaget denne henstilling. Denne henstilling beskriver en række trin, som eksportører kan følge, mulige informationskilder og nogle eksempler på supplerende foranstaltninger, der kan indføres.

Som **første trin** anbefaler Databeskyttelsesrådet jer, eksportører, at **kende jeres overførsler**. Kortlægning af alle overførsler af personoplysninger til tredjelande kan være svært. Det er imidlertid nødvendigt at være opmærksom på, hvor personoplysninger overføres til, for at sikre at de ydes en beskyttelse, der i det væsentlige er tilsvarende, uanset hvor de bliver behandlet. I skal også verificere, om de oplysninger, I overfører, er tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles.

Et **andet trin** er at **verificere det overførselsværktøj, jeres overførsler afhænger af**, blandt dem, der er nævnt i kapitel V i GDPR. Hvis Europa-Kommissionen allerede har erklæret det land, den region eller den sektor, I overfører oplysningerne til, for tilstrækkelig ved en afgørelse om tilstrækkelighed i medfør af artikel 45 i GDPR eller i medfør af det tidligere direktiv 95/46, såfremt afgørelsen stadig er gyldig, behøver I ikke at foretage jer yderligere, bortset fra at føre tilsyn med, om afgørelsen om tilstrækkelighed fortsat er gyldig. Hvis der ikke foreligger en afgørelse om tilstrækkelighed, skal I benytte et af de overførselsværktøjer, der er nævnt i artikel 46 i GDPR. Kun i nogle tilfælde kan I eventuelt henholde jer til en af undtagelserne i artikel 49 i GDPR, hvis I opfylder betingelserne. Undtagelser kan ikke blive "reglen" i praksis, men skal begrænses til særlige situationer.

Et **tredje trin** er at **vurdere**, om der er noget i tredjelandets lovgivning og/eller gældende praksis, der kan kollidere med effektiviteten af de fornødne garantier ved de overførselsværktøjer, I benytter i forbindelse med den konkrete overførsel. Vurderingen bør først og fremmest være koncentreret om den del af tredjelandets lovgivning, der er relevant for overførslen og det overførselsværktøj, jf. artikel 46 i GDPR, I benytter. En undersøgelse af tredjelandets offentlige myndigheders praksis vil ligeledes gøre det muligt for jer at verificere, om garantiene i overførselsværktøjet i praksis kan sikre en effektiv beskyttelse af de overførte personoplysninger. En undersøgelse af denne praksis vil navnlig være relevant for vurderingen, hvis:

(i.) lovgivning i tredjelandet, der formelt opfylder EU's standarder, åbenbart ikke anvendes/overholdes i praksis

(ii.) der foreligger praksis, som er uforenelig med tilsagnene i overførselsværktøjet, hvis der mangler relevant lovgivning i tredjelandet

(iii.) jeres overførte oplysninger og/eller importør er eller kan være omfattet af anvendelsesområdet for problematisk lovgivning (dvs. kan bringe overførselsværktøjets kontraktlige garanti for et i det væsentlige tilsvarende beskyttelsesniveau i fare og opfylder ikke EU's standarder vedrørende grundlæggende rettigheder, nødvendighed og proportionalitet).

I de første to situationer vil I skulle suspendere overførslen eller gennemføre passende supplerende foranstaltninger, hvis I ønsker at gå videre med den.

I den tredje situation kan I i lyset af usikkerheden med hensyn til en eventuel anvendelse af problematisk lovgivning på jeres overførsel beslutte at: suspendere overførslen, gennemføre supplerende foranstaltninger for at gå videre med den, eller I kan alternativt beslutte at gå videre med overførslen uden at gennemføre supplerende foranstaltninger, hvis I vurderer og kan påvise og dokumentere, at I ikke har nogen grund til at tro, at den relevante og problematiske lovgivning vil blive fortolket og/eller i praksis anvendt på jeres overførte oplysninger og importør.

Til evaluering af de elementer, der skal tages i betragtning ved vurdering af et tredjelandets lovgivning om offentlige myndigheders adgang til oplysninger i forbindelse med overvågning, henvises til Databeskyttelsesrådets henstilling om europæiske væsentlige garantier.

Denne vurdering bør udføres med fornøden omhu og dokumenteres grundigt. De kompetente tilsynsmyndigheder og/eller retlige myndigheder kan anmode herom og drage jer til ansvar for enhver beslutning, I træffer på dette grundlag.

Et **fjerde trin** er at **udpege og vedtage supplerende foranstaltninger**, der er nødvendige for at bringe beskyttelsesniveauet for overførte oplysninger på linje med EU-standard for væsentlig overensstemmelse. Dette trin er kun nødvendigt, hvis jeres vurdering viser, at tredjelandets lovgivning og/eller praksis kolliderer med effektiviteten af det overførselsværktøj, jf. artikel 46 i GDPR, I benytter, eller I har til hensigt at benytte i forbindelse med overførslen. Denne henstilling indeholder (i bilag 2) en ikke-udtømmende liste over eksempler på supplerende foranstaltninger og nogle af de betingelser, som de ville kræve for at være effektive. På samme måde som med de fornødne garantier i overførselsværktøjerne, jf. artikel 46, kan nogle supplerende foranstaltninger være effektive i nogle lande, men ikke nødvendigvis i andre. I vil være ansvarlige for at vurdere effektiviteten af dem i forbindelse med overførslen og i lyset af tredjelandets lovgivning og praksis samt det overførselsværktøj, I benytter, da I bliver draget til ansvar for enhver beslutning, I træffer på dette grundlag. Dette kan også forudsætte, at I kombinerer flere supplerende foranstaltninger. I sidste ende kan jeres konklusion blive, at der ikke er nogen supplerende foranstaltning, der kan sikre et beskyttelsesniveau, der i det væsentlige er tilsvarende, for den konkrete overførsel. I de tilfælde, hvor der ikke er nogen passende supplerende foranstaltning, skal I forhindre, suspendere eller indstille overførslen for ikke at kompromittere niveauet for beskyttelse af personoplysninger. Denne vurdering af supplerende foranstaltninger bør ligeledes udføres med fornøden omhu og dokumenteres.

Et **femte trin** er at **indføre** eventuelle **formelle tiltag**, som måtte være nødvendige som følge af vedtagelsen af den supplerende foranstaltning, afhængigt af det overførselsværktøj, jf. artikel 46 i GDPR, I benytter. I denne henstilling specificeres nogle af disse formaliteter. I kan få behov for at konsultere de kompetente tilsynsmyndigheder vedrørende nogle formaliteter.

Det **sjette og sidste trin** er med passende intervaller at **gentage vurderingen** af beskyttelsesniveauet for de personoplysninger, I overfører til tredjelande, og holde øje med, om der har været eller kommer en udvikling, som kan påvirke niveauet. Ansvarlighedsprincippet kræver løbende overvågning af niveauet for beskyttelse af personoplysninger.

Tilsynsmyndigheder vil løbende udøve deres mandat til at overvåge anvendelsen af GDPR og til at håndhæve den. Tilsynsmyndigheder ser navnlig på de tiltag, eksportører træffer, for at sikre, at de oplysninger, de overfører, har et beskyttelsesniveau, der i det væsentlige svarer til det i GDPR. Som Domstolen påpeger, vil tilsynsmyndigheder suspendere eller forbyde dataoverførsler i disse tilfælde, hvis de efter en undersøgelse eller klage konkluderer, at der ikke kan sikres et beskyttelsesniveau, der i det væsentlige er tilsvarende.

Tilsynsmyndigheder vil fortsat udarbejde vejledninger til eksportører og koordinere deres indsats i Databeskyttelsesrådet for at sikre en konsekvent anvendelse af EU's databeskyttelseslovgivning.

INDHOLDSFORTEGNELSE

Indholdsfortegnelse	6
1 Ansvarlighed i overførsler af oplysninger	9
2 Køreplan: anvendelse af ansvarlighedsprincippet ved dataoverførsler i praksis	10
2.1 Trin 1: Kend jeres overførsler	10
2.2 Trin 2: Fastlæg de overførselsværktøjer, I benytter	12
2.3 Trin 3: Vurder, om det overførselsværktøj i artikel 46 i GDPR, I benytter, er effektivt i lyset af omstændighederne vedrørende overførslen	15
2.4 Trin 4: Vedtag supplerende foranstaltninger	23
2.5 Trin 5: Proceduremæssige trin, hvis I har fastlagt effektive supplerende foranstaltninger ..	26
2.6 Trin 6: Gentag evalueringen med passende mellemrum	27
3 Konklusion	28
Bilag 1: DEFINITIONER	29
BILAG 2: EKSEMPLER PÅ SUPPLERENDE FORANSTALTNINGER	30
2.1 Tekniske foranstaltninger	30
2.2 Yderligere kontraktmæssige foranstaltninger	39
2.3 Organisatoriske foranstaltninger	48
BILAG 3: MULIGE INFORMATIONSKILDER TIL VURDERING af et tredjeland	52

Det Europæiske Databeskyttelsesråd har —

under henvisning til artikel 70, stk. 1, litra e), i Europa-Parlamentets og Rådets forordning 2016/679/EU af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (i det følgende benævnt "GDPR"),

under henvisning til aftalen om Det Europæiske Økonomiske Samarbejdsområde (EØS), særlig bilag XI og protokol 37 til EØS-aftalen, som ændret ved Det Blandede EØS-Udvalgs afgørelse nr. 154/2018 af 6. juli 2018¹,

under henvisning til artikel 12 og artikel 22 i forretningsordenen og

ud fra følgende betragtninger:

(1) Den Europæiske Unions Domstol (EU-Domstolen) konkluderer i sin dom af 16. juli 2020 *Data Protection Commissioner mod Facebook Ireland LTD og Maximillian Schrems*, C-311/18, at artikel 46, stk. 1, og artikel 46, stk. 2, litra c), i GDPR skal fortolkes således, at de fornødne garantier, de rettigheder, som kan håndhæves, og de effektive retsmidler, som kræves ved disse bestemmelser, skal sikre, at der for de rettigheder, som tilkommer personer, hvis oplysninger overføres til et tredjeland på grundlag af standardbestemmelser om databeskyttelse, gælder et beskyttelsesniveau, der i det væsentlige svarer til det niveau, der er sikret i Unionen ved denne forordning, sammenholdt med Den Europæiske Unions charter om grundlæggende rettigheder.²

(2) Som EU-Domstolen understregede, skal fysiske personer sikres et beskyttelsesniveau, der i det væsentlige svarer til det, der er sikret i Unionen ved GDPR læst i sammenhæng med chartret, uanset bestemmelsen i kapitel V, som danner grundlag for en overførsel af personoplysninger til et tredjeland. Formålet med bestemmelserne i kapitel V er at sikre opretholdelsen af det høje niveau for denne beskyttelse ved overførsel af personoplysninger til et tredjeland.³

(3) Betragtning 108 og artikel 46, stk. 1, i GDPR fastslår, at i mangel af en EU-afgørelse om tilstrækkelighed bør en dataansvarlig eller databehandler træffe foranstaltninger for at kompensere for den manglende databeskyttelse i et tredjeland i form af fornødne garantier for den registrerede. En dataansvarlig eller databehandler kan give de fornødne garantier uden krav om en specifik godkendelse fra en tilsynsmyndighed ved at benytte et af de overførselsværktøjer, der er nævnt i artikel 46, stk. 2, i GDPR, f.eks. standardbestemmelser om databeskyttelse.

(4) EU-Domstolen præciserer, at de af Kommissionen vedtagne standardbestemmelser om databeskyttelse alene tager sigte på at give dataansvarlige eller databehandlere, som er etableret i

¹ Henvisninger til "medlemsstater" i dette dokument skal forstås som henvisninger til "EØS-medlemsstater".

² EU-Domstolens dom af 16. juli 2020, *Data Protection Commissioner mod Facebook Ireland Ltd og Maximillian Schrems*, (i det følgende benævnt C-311/18 (Schrems II)), anden konstatering.

³ C-311/18 (Schrems II), præmis 92 og 93.

Unionen, kontraktlige garantier, der anvendes ens i alle tredjelande. På grund af standardbestemmelser om databeskyttelses kontraktlige karakter kan de ikke binde offentlige myndigheder i tredjelande, eftersom de ikke er part i kontrakten. Derfor kan dataeksportører være nødt til at supplere garantierne i disse standardbestemmelser om databeskyttelse med supplerende foranstaltninger for at sikre opfyldelse af det beskyttelsesniveau, der kræves i EU-retten, i et bestemt tredjeland. EU-Domstolen henviser til betragtning 109 i GDPR, der nævner denne mulighed og tilskynder dataansvarlige og databehandlere til at bruge den.⁴

(5) Domstolen slog fast, at det først og fremmest tilkommer dataeksportøren i hvert enkelt tilfælde og, hvor det er relevant i samarbejde med dataimportøren, at undersøge, om lovgivningen i bestemmelseslandet sikrer et beskyttelsesniveau, der i det væsentlige svarer til niveauet i EU-retten af de personoplysninger, som overføres på grundlag af standardbestemmelser om databeskyttelse, ved efter behov at give supplerende garantier i forhold til de garantier, som disse bestemmelser yder.⁵

(6) Hvis den dataansvarlige eller en databehandler, som er etableret i Unionen, ikke er i stand til at træffe supplerende foranstaltninger, som sikrer et beskyttelsesniveau, der i det væsentlige svarer til niveauet i EU-retten, skal de, eller subsidiært den kompetente tilsynsmyndighed, suspendere eller indstille overførslen af personoplysninger til det pågældende tredjeland.⁶

(7) Hverken GDPR eller Domstolen definerer eller specificerer "yderligere garantier", "yderligere foranstaltninger" eller "supplerende foranstaltninger" med hensyn til garantien ved de overførselsværktøjer, der er opført i artikel 46, stk. 2, i GDPR, som dataansvarlige og databehandlere kan vedtage for sikre overholdelse af det beskyttelsesniveau, der kræves i henhold til EU-retten, i et bestemt tredjeland.

(8) Databeskyttelsesrådet har på eget initiativ besluttet at undersøge dette spørgsmål og komme med henstillinger til dataansvarlige og databehandlere, der fungerer som eksportører, om procedurer, de kan følge for at udpege og vedtage supplerende foranstaltninger. Formålet med disse henstillinger er at give eksportører en metode til at afgøre, om der er behov for yderligere foranstaltninger, og i givet fald hvilke der skal indføres vedrørende deres overførsler. Det er primært eksportørers ansvar at sikre, at de overførte oplysninger i tredjelandet sikres et beskyttelsesniveau, der i det væsentlige svarer til det niveau, der er sikret i EØS. Databeskyttelsesrådet ønsker i medfør af sit mandat med disse henstillinger at tilskynde til en ensartet anvendelse af GDPR og Domstolens afgørelse⁷ —

VEDTAGET FØLGENDE HENSTILLINGER:

⁴ C-311/18 (Schrems II), præmis 132 og 133.

⁵ C-311/18 (Schrems II), præmis 134.

⁶ C-311/18 (Schrems II), præmis 135.

⁷ Artikel 70, stk. 1, litra e), i GDPR.

1 ANSVARLIGHED I OVERFØRSLER AF OPLYSNINGER

1. Primærretten i EU anser retten til databeskyttelse for en grundlæggende rettighed.⁸ Retten til databeskyttelse sikres derfor med et højt beskyttelsesniveau, og der kan kun indrømmes begrænsninger, hvis de har hjemmel i lovgivningen, respekterer det væsentligste indhold af retten, er forholdsmæssige, nødvendige og faktisk opfylder formålene af generel interesse, som Unionen har anerkendt, eller behovet for at beskytte andres rettigheder og frihedsrettigheder.⁹ Retten til beskyttelse af personoplysninger skal ses i sammenhæng med sin funktion i samfundet og afvejes i forhold til andre grundlæggende rettigheder i overensstemmelse med proportionalitetsprincippet.¹⁰
2. Oplysninger skal beskyttes på et niveau, der i det væsentlige svarer til den beskyttelse, der er sikret i EU, når de overføres til tredjelande uden for EØS for at sikre, at det beskyttelsesniveau, der er sikret ved GDPR, ikke undermineres, både under og efter overførslen.
3. Retten til databeskyttelse har en aktiv karakter. Den kræver, at eksportører og importører (uanset om de er dataansvarlige og/eller databehandlere) går videre end en erkendelse af eller passiv overholdelse af denne rettighed.¹¹ Dataansvarlige og databehandlere skal aktivt og løbende opfylde retten til databeskyttelse ved at gennemføre juridiske, tekniske og organisatoriske foranstaltninger, der sikrer rettens effektivitet. Dataansvarlige og databehandlere skal desuden kunne påvise deres bestræbelser over for registrerede og tilsynsmyndighederne for databeskyttelse. Dette er det såkaldte ansvarlighedsprincip.¹²
4. Ansvarlighedsprincippet, som er nødvendigt for at sikre effektiv anvendelse af det beskyttelsesniveau, der ydes af GDPR, finder også anvendelse på dataoverførsler til tredjelande¹³, eftersom disse i sig selv er en form for databehandling.¹⁴ Som Domstolen understregede i sin dom, skal der sikres et beskyttelsesniveau, som i det væsentlige svarer til det, der er sikret i Unionen ved GDPR læst i sammenhæng med chartret, uanset bestemmelsen i det kapitel, som danner grundlag for en overførsel af personoplysninger til et tredjeland.¹⁵
5. I Schrems II-dommen understreger Domstolen eksportørers og importørers ansvar for at sikre, at behandlingen af personoplysninger er blevet og fortsat vil blive udført i overensstemmelse med det beskyttelsesniveau, der er fastsat i EU's databeskyttelseslovgivning, og at suspendere overførslen og/eller ophæve kontrakten, hvis importøren af oplysningerne ikke længere er i stand til at opfylde standardbestemmelser om databeskyttelse, der er indarbejdet i den pågældende

⁸ Artikel 8, stk. 1, i chartret om grundlæggende rettigheder og artikel 16, stk. 1, i TEUF, præambel 1, artikel 1, stk. 2, i GDPR.

⁹ Artikel 52, stk. 1, i EU's charter om grundlæggende rettigheder.

¹⁰ Betragtning 4 i GDPR og C-507/17 Google LLC, indtrådt i Google Inc.'s rettigheder mod Commission nationale de l'informatique et des libertés (CNIL), præmis 60.

¹¹ C-92/09 og C-93/02, Volker und Markus Schecke GbR mod Land Hessen, forslag til afgørelse fra generaladvokat Sharpston, 17. juni 2010, præmis 71.

¹² Artikel 5, stk. 2, og artikel 28, stk. 3, litra h), i GDPR.

¹³ Artikel 44 og betragtning 101 i GDPR samt artikel 47, stk. 2, litra d), i GDPR.

¹⁴ EU-Domstolens dom af 6. oktober 2015, *Maximilian Schrems mod Data Protection Commissioner*, (i det følgende benævnt C-362/14 (Schrems I)), præmis 45.

¹⁵ C-311/18 (Schrems II), præmis 92 og 93.

kontrakt mellem eksportøren og importøren.¹⁶ Den dataansvarlige eller databehandleren, der fungerer som eksportør, skal sikre, at importørerne, når det er relevant, samarbejder med eksportøren om dennes varetagelse af sit ansvar ved f.eks. at underrette eksportøren om al udvikling, der påvirker niveauet for beskyttelse af personoplysninger, der modtages i importørens land.¹⁷ Dette ansvar er en anvendelse af ansvarlighedsprincippet for dataoverførsler i GDPR.¹⁸

2 KØREPLAN: ANVENDELSE AF ANSVARLIGHEDSPRINCIPPET VED DATAOVERFØRSLER I PRAKSIS

6. I det følgende beskrives en køreplan med de trin, der skal følges for at afgøre, om I (dataeksportører) skal indføre supplerende foranstaltninger for lovligt at kunne overføre oplysninger til lande uden for EØS. "I" vil i dette dokument sige dataansvarlige eller databehandlere, der fungerer som dataeksportører¹⁹ og behandler personoplysninger inden for GDPR's anvendelsesområde — herunder private enheder og offentlige organer, der behandler oplysninger, når de overfører dem til private organer.²⁰ For så vidt angår overførsler af personoplysninger mellem offentlige organer er der specifikke retningslinjer i *Retningslinjer 2/2020 om artikel 46, stk. 2, litra a), og artikel 46, stk. 3, litra b), i forordning 2016/679 om overførsler af personoplysninger mellem offentlige myndigheder og organer i og uden for EØS*.²¹
7. I skal kunne dokumentere denne vurdering og de supplerende foranstaltninger, I vælger og gennemfører, behørigt og efter anmodning stille denne dokumentation til rådighed for den kompetente tilsynsmyndighed.²²

2.1 Trin 1: Kend jeres overførsler

8. For at vide, hvad der kræves af jer (dataeksportører) for at kunne fortsætte med eller foretage nye overførsler af personoplysninger,²³ er første trin at sikre, at I har et grundigt kendskab til jeres overførsler (kend jeres overførsler). Registrering og kortlægning af alle overførsler kan være en kompleks øvelse for enheder, der foretager mange, forskelligartede og regelmæssige overførsler til tredjelande, og som benytter en række databehandlere samt underdatabehandlere. At kende

¹⁶ C-311/18 (Schrems II), præmis 134, 135, 139, 140, 141 og 142.

¹⁷ C-311/18 (Schrems II), præmis 134.

¹⁸ Artikel 5, stk. 2, og artikel 28, stk. 3, litra h), i GDPR.

¹⁹ Derfor vil man eksempelvis ikke blive betragtet som en dataeksportør, hvis man er en registreret, der via et onlinespørgeskema videregiver sine personoplysninger til en dataansvarlig, der er etableret i et tredjeland.

²⁰ Se Databeskyttelsesrådets retningslinjer 3/2018 om det territoriale anvendelsesområde for databeskyttelsesforordningen (artikel 3) <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version-en>

²¹ Databeskyttelsesrådets retningslinjer 2/2020 om artikel 46, stk. 2, litra a), og artikel 46, stk. 3, litra b), i forordning 2016/679 om overførsler af personoplysninger mellem offentlige myndigheder og organer i og uden for EØS, se <https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b-en>

²² Artikel 5, stk. 2, og artikel 24, stk. 1), i GDPR.

²³ Vær opmærksom på, at en enhed fra et tredjelands fjernadgang til oplysninger, der befinder sig i EØS, også anses for en overførsel.

jeres overførsler er et vigtigt første trin i opfyldelsen af jeres forpligtelser under ansvarlighedsprincippet.

9. For at få et indgående kendskab til jeres overførsler kan I trække på fortegnelser over behandlingsaktiviteter, som I eventuelt kan være forpligtede til at føre i medfør af artikel 30 i GDPR.²⁴ Tidligere handlinger, der har til formål at opfylde pligten til at informere registrerede, jf. artikel 13, stk. 1, litra f), og artikel 14, stk. 1, litra f), i GDPR, om jeres overførsler af deres personoplysninger til tredjelande, kan også hjælpe jer.²⁵
10. Ved kortlægning af overførsler skal I huske også at tage videreoverførsler i betragtning, f.eks. hvis jeres databehandlere uden for EØS overfører de personoplysninger, I har overdraget dem, til en underdatabehandler i et tredjeland eller i samme tredjeland.²⁶
11. I tråd med GDPR-princippet om "dataminimering"²⁷ skal I også verificere, at de oplysninger, I overfører, er tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles.
12. Disse aktiviteter skal udføres, før der foretages en overførsel, og de skal opdateres, før overførsler genoptages efter suspendering af dataoverførselsaktiviteter: I skal vide, hvor de personoplysninger, I eksporterede, kan befinde sig eller blive behandlet af importørerne (kort over destinationer).
13. Vær opmærksom på, at fjernadgang fra et tredjeland (f.eks. i forbindelse med support) og/eller lagring i en cloud, der befinder sig uden for EØS og udbydes af en tjenesteudbyder, også betragtes som en overførsel.²⁸ Hvis I benytter en international cloud-infrastruktur, skal I konkret vurdere, om oplysningerne bliver overført til tredjelande og hvilke, medmindre cloud-udbyderen er etableret i EØS og i sin kontrakt tydeligt erklærer, at oplysningerne slet ikke bliver behandlet i tredjelande.

²⁴ Jf. artikel 30 i GDPR, særlig stk. 1, litra e), og stk. 2, litra c). Desuden bør jeres fortegnelser over behandling indeholde en beskrivelse af behandlingsaktiviteterne (herunder men ikke begrænset til kategorier af registrerede, kategorier af personoplysninger samt formål med behandlingen og specifikke oplysninger om dataoverførslerne. Nogle dataansvarlige og databehandlere er undtaget fra pligten til at føre fortegnelser over behandling (artikel 30, stk. 5, i GDPR). For retningslinjer om denne undtagelse henvises til Artikel 29-Gruppens holdningsdokument om undtagelser fra pligten til at føre fortegnelser over behandlingsaktiviteter i henhold til artikel 30, stk. 5, i GDPR (som Databeskyttelsesrådet tilsluttede sig den 25. maj 2018).

²⁵ I henhold til gennemsigtighedsbestemmelserne i GDPR skal I underrette registrerede om overførsler af personoplysninger til tredjelande (artikel 13, stk. 1, litra f), og artikel 14, stk. 1, litra f), i GDPR). I skal navnlig underrette dem om, hvorvidt der foreligger en afgørelse om tilstrækkelighed truffet af Europa-Kommissionen, eller for så vidt angår overførsler, der er omtalt i artikel 46 eller 47 i GDPR, eller artikel 49, stk. 1, andet afsnit, i GDPR, henviser til de fornødne eller passende garantier, og hvordan de kan få en kopi af dem, eller hvor de er blevet stillet til rådighed. Oplysningerne, der gives til den registrerede, skal være korrekte og ajourførte, navnlig med hensyn til Domstolens retspraksis om overførsler.

²⁶ Hvis den dataansvarlige har givet sin forudgående specifikke eller generelle skriftlige godkendelse, jf. artikel 28, stk. 2, i GDPR.

²⁷ Artikel 5, stk. 1, litra c), i GDPR.

²⁸ Se ofte stillede spørgsmål nr. 11 "det bør påpeges, at hvis der gives adgang til oplysninger fra et tredjeland, f.eks. i forbindelse med administration, er dette også en overførsel", Databeskyttelsesrådets ofte stillede spørgsmål om Den Europæiske Unions Domstols dom i sagen C-311/18 — Data Protection Commissioner mod Facebook Ireland Ltd og Maximilian Schrems, af 23. juli 2020.

2.2 Trin 2: Fastlæg de overførselsværktøjer, I benytter

14. Det andet trin, I skal udføre, er at fastlægge de overførselsværktøjer, I benytter, blandt dem, der er nævnt i kapitel V i GDPR.

Afgørelser om tilstrækkelighed

15. Europa-Kommissionen kan ved sine **afgørelser om tilstrækkelighed** afgøre, om nogle eller alle de tredjelande, I overfører personoplysninger til, yder et tilstrækkeligt niveau for beskyttelse af personoplysninger.²⁹
16. Virkningen af en sådan afgørelse om tilstrækkelighed er, at personoplysninger kan strømme fra EØS til det pågældende tredjeland uden behov for nogle af de i artikel 46 i GDPR omtalte overførselsværktøjer.
17. Afgørelser om tilstrækkelighed kan omfatte et helt land eller være begrænset til en del af det. Afgørelser om tilstrækkelighed kan omfatte alle dataoverførsler til et land eller være begrænset til nogle typer af overførsler (f.eks. i en sektor).³⁰
18. Europa-Kommissionen offentliggør listen over afgørelser om tilstrækkelighed på sit websted.³¹
19. Hvis I overfører personoplysninger til tredjelande, regioner eller sektorer, der er omfattet af en afgørelse om tilstrækkelighed fra Kommissionen (i det omfang den er gældende), **behøver I ikke træffe nogen af de yderligere foranstaltninger, der er beskrevet i denne henstilling**.³² I skal dog stadig holde øje med, om de afgørelser om tilstrækkelighed, der er relevante for jeres overførsler, bliver trukket tilbage eller kendt ugyldige.³³
20. Afgørelser om tilstrækkelighed kan imidlertid ikke forhindre registrerede i at indgive en klage. De forhindrer heller ikke tilsynsmyndigheder i at anlægge sag for en national domstol, hvis de er i tvivl om gyldigheden af en afgørelse, således at en national domstol kan forelægge en anmodning om præjudiciel afgørelse for EU-Domstolen med henblik på en efterprøvelse af dennes gyldighed.³⁴

²⁹ Europa-Kommissionen har i medfør af artikel 45 i GDPR bemyndigelse til at afgøre, om et land uden for EU yder et tilstrækkeligt databeskyttelsesniveau. Europa-Kommissionen har ligeledes bemyndigelse til at afgøre, om en international organisation yder et tilstrækkeligt beskyttelsesniveau.

³⁰ Artikel 45, stk. 1, i GDPR.

³¹ https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

³² Forudsat at I og dataimportøren har gennemført foranstaltninger til at opfylde de øvrige forpligtelser i GDPR, ellers skal disse foranstaltninger gennemføres.

³³ Europa-Kommissionen skal regelmæssigt revidere alle afgørelser om tilstrækkelighed og overvåge, om tredjelande omfattet af afgørelser om tilstrækkelighed fortsat sikrer et tilstrækkeligt beskyttelsesniveau (jf. artikel 45, stk. 3, og artikel 45, stk. 4, i GDPR). Desuden kan EU-Domstolen kende afgørelser om tilstrækkelighed ugyldige (jf. dommene i sagerne C-362/14 (Schrems I) og C-311/18 (Schrems II)).

³⁴ C-311/18 (Schrems II), præmis 118-120. Tilsynsmyndigheder må ikke se bort fra afgørelsen om tilstrækkelighed og suspendere eller forbyde overførsler af personoplysninger til sådanne lande alene under påberåbelse af beskyttelsesniveauets utilstrækkelighed. De må kun udøve deres beføjelse til at suspendere eller forbyde

Eksempel:

En EU-borger, Maximillian Schrems, indgav en klage i juni 2013 mod Irish Data Protection Commission (DPC) og anmodede denne tilsynsmyndighed om at forbyde eller suspendere overførslen af hans personoplysninger fra Facebook Ireland til USA, fordi han mente, at USA's lovgivning og praksis ikke sikrede tilstrækkelig beskyttelse af de personoplysninger, der opbevares på landets område, mod den overvågningsvirksomhed, som de offentlige myndigheder udøvede dér. DPC afviste klagen navnlig med den begrundelse, at Kommissionen i beslutning 2000/520 havde fastslået, at USA under "safe harbour"-ordningen sikrede et tilstrækkeligt niveau for beskyttelse af personoplysninger (safe harbour-beslutningen). Maximillian Schrems anfægtede DPC's afgørelse, og Irish High Court forelagde et spørgsmål om gyldigheden af beslutning 2000/520 for Den Europæiske Unions Domstol (EU-Domstolen). EU-Domstolen besluttede efterfølgende at kende Kommissionens beslutning 2000/520 om tilstrækkeligheden af den beskyttelse, der opnås ved hjælp af safe harbour-principperne til beskyttelse af privatlivets fred, ugyldig.³⁵

overførsler af personoplysninger til det pågældende tredjeland med andre begrundelser (f.eks. utilstrækkelige sikkerhedsforanstaltninger i strid med artikel 32 i GDPR, manglende retsgrundlag som gyldigt grundlag for databehandlingen i strid med artikel 6 i GDPR). Tilsynsmyndigheder kan fuldstændig uafhængigt undersøge, om overførslen af oplysninger overholder kravene i GDPR, og hvis det er relevant, indbringe en sag for de nationale domstole, hvis de er i tvivl om gyldigheden af Kommissionens afgørelse om tilstrækkelighed for at forelægge en anmodning om præjudiciel afgørelse for EU-Domstolen med henblik på en efterprøvelse af dennes gyldighed.

³⁵ Sag C-362/14 (Schrems I).

Overførselsværktøjer, jf. artikel 46 i GDPR

21. I artikel 46 i GDPR er der nævnt en række overførselsværktøjer, der indeholder "*fornødne garantier*", og som eksportører kan benytte til at overføre personoplysninger til tredjelande, hvis der ikke foreligger en afgørelse om tilstrækkelighed. De vigtigste typer overførselsværktøjer i artikel 46 i GDPR er:
- standardbestemmelser om databeskyttelse
 - bindende virksomhedsregler
 - adfærdskodekser
 - certificeringsmekanismer
 - ad hoc-kontraktbestemmelser.
22. Uanset hvilket overførselsværktøj i artikel 46 i GDPR I vælger, skal I generelt sikre, at de overførte personoplysninger er omfattet af et beskyttelsesniveau, der i det væsentlige svarer til niveauet i GDPR.
23. Overførselsværktøjerne, jf. artikel 46 i GDPR, indeholder primært *fornødne garantier* af kontraktlig art, der kan anvendes på overførsler til alle tredjelande. Det kan på baggrund af situationen i det tredjeland, I overfører oplysninger til, stadig være nødvendigt, at I supplerer disse overførselsværktøjer og garantierne heri med yderligere foranstaltninger ("*supplerende foranstaltninger*") for at sikre et beskyttelsesniveau, der i det væsentlige svarer til niveauet i GDPR.³⁶

Undtagelser

24. Udover afgørelser om tilstrækkelighed og de i artikel 46 i GDPR omtalte overførselsværktøjer indeholder GDPR en tredje metode til overførsler af personoplysninger i visse situationer. I henhold til særlige betingelser kan I stadig overføre personoplysninger på grundlag af en af de i artikel 49 i GDPR nævnte undtagelser.
25. Artikel 49 i GDPR er af ekstraordinær karakter. Undtagelserne heri skal fortolkes på en måde, der ikke er i strid med undtagelsernes karakter af undtagelser fra reglen om, at personoplysninger ikke må overføres til et tredjeland, medmindre landet sikrer et tilstrækkeligt databeskyttelsesniveau eller indfører de *fornødne garantier*. Undtagelser kan ikke blive "*reglen*" i praksis, men skal begrænses til særlige situationer. Databeskyttelsesrådet har udstedt retningslinjer 2/2018 vedrørende undtagelser i artikel 49 i forordning 2016/679.³⁷
26. Før I henholder jer til en undtagelse i artikel 49 i GDPR, skal I tjekke, om jeres overførsel opfylder de strenge betingelser, som denne bestemmelse fastlægger for hver undtagelse.

³⁶ C-311/18 (Schrems II), præmis 130 og 133. Se desuden underafsnit 2.3 herunder.

³⁷ For yderligere retningslinjer herom henvises til https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en.

27. Hvis jeres overførsel hverken kan begrundes juridisk i en afgørelse om tilstrækkelighed eller i en undtagelse i artikel 49, skal I fortsætte med trin 3.

2.3 Trin 3: Vurder, om det overførselsværktøj i artikel 46 i GDPR, I benytter, er effektivt i lyset af omstændighederne vedrørende overførslen

28. Det valgte overførselsværktøj i artikel 46 GDPR skal effektivt kunne sikre, at det beskyttelsesniveau, der er sikret ved GDPR, ikke undermineres ved overførslen i praksis.³⁸

29. Navnlig skal beskyttelsen af de overførte personoplysninger i tredjelandet i det væsentlige svare til den beskyttelse, der er sikret i EØS ved GDPR, sammenholdt med EU's charter om grundlæggende rettigheder.³⁹ Dette er ikke tilfældet, hvis dataimportøren på grund af lovgivningen og praksis i tredjelandet, der finder anvendelse på overførslen, er forhindret i at opfylde sine forpligtelser i henhold til det valgte overførselsværktøj, jf. artikel 46 i GDPR, herunder i forbindelse med oplysningers transit fra eksportøren til importørens land.⁴⁰

30. I skal først vurdere, hvor det er relevant i samarbejde med importøren, om der er noget i lovgivningen og/eller gældende praksis⁴¹ i tredjelandet, der kan kollidere med effektiviteten af de fornødne garantier ved de overførselsværktøjer, jf. artikel 46 i GDPR, I benytter, i forbindelse med den konkrete overførsel. Det skal herved afgøres, om overførslen er omfattet af anvendelsesområdet for lovgivning og/eller praksis, der kan påvirke effektiviteten af jeres overførselsværktøj, jf. artikel 46 i GDPR. Den krævede vurdering skal først og fremmest være baseret på den offentligt tilgængelige lovgivning.

31. Denne vurdering skal indeholde elementer vedrørende adgang til oplysninger for offentlige myndigheder i jeres importørs tredjeland, såsom:

- Elementer med hensyn til, om offentlige myndigheder i jeres importørs tredjeland kan søge at opnå adgang til oplysningerne med eller uden dataimportørens viden, på baggrund af lovgivning, praksis og tidligere rapporterede hændelser
- Elementer med hensyn til, om offentlige myndigheder i jeres importørs tredjeland kan være i stand til at opnå adgang til oplysningerne via dataimportøren eller via telekommunikationsudbyderne eller kommunikationskanalerne, på baggrund af lovgivning, juridiske beføjelser, de tekniske, finansielle og menneskelige ressourcer, der er til deres rådighed, samt tidligere rapporterede hændelser.

Kortlægning af lovgivning og praksis, der er relevant i lyset af omstændighederne vedrørende overførslen

32. I skal se nærmere på karakteristikaene for hver overførsel og afgøre, om retssystemet og/eller gældende praksis i det land, oplysningerne overføres til (eller videreoverføres til), påvirker jeres overførsler. Jeres vurdering er således begrænset til den lovgivning og praksis, der er relevant for

³⁸ Artikel 44 i GDPR og præmis 126, 137 og 148 i C-311/18 (Schrems II).

³⁹ C-311/18 (Schrems II), præmis 105 og anden konstatering.

⁴⁰ Jf. C-311/18 (Schrems II), præmis 183 sammenholdt med præmis 184.

⁴¹ Jf. præmis 126 i C-311/18 (Schrems II), hvor Domstolen udtrykkeligt henviser til "retstilstanden og gældende praksis i det pågældende tredjeland" og kræver sikring af "(...) den effektive beskyttelse af de personoplysninger, som er overført til det pågældende tredjeland, i praksis." (fremhævelse tilføjet), og præmis 158.

beskyttelsen af de specifikke oplysninger, I overfører, i modsætning til de generelle og omfattende vurderinger af tilstrækkelighed, Europa-Kommissionen udfører i henhold til artikel 45 i GDPR.

33. Den gældende retlige baggrund og/eller praksis afhænger af de specifikke omstændigheder for jeres overførsel, især:
- formålene med overførslen og behandlingen af oplysningerne (f.eks. markedsføring, personale, lagring, IT-støtte, kliniske forsøg)
 - typer af enheder involveret i behandlingen (offentlige/private, dataansvarlig/databehandler)
 - den sektor, hvor overførslen finder sted (f.eks. adtech, telekommunikation, finans osv.)
 - kategorier af overførte personoplysninger (f.eks. kan personoplysninger vedrørende børn være omfattet af særlig lovgivning i tredjelandet)⁴²
 - om oplysningerne bliver lagret i tredjelandet, eller om der er tale om fjernadgang til oplysninger lagret i EU/EØS
 - format af oplysningerne, der skal overføres (f.eks. almindelig tekst/pseudonymiseret eller krypteret)⁴³
 - mulighed for, at oplysninger kan blive videreoverført fra tredjelandet til et andet tredjeland.⁴⁴
34. Jeres vurdering bør tage alle aktører, der deltager i overførslen (f.eks. dataansvarlige, databehandlere og underbehandlere, der behandler oplysninger i tredjelandet), og som blev udpeget i forbindelse med kortlægningen af overførslerne, i betragtning. Jo flere dataansvarlige, databehandlere eller dataimportører, der er involveret, jo mere kompleks bliver jeres vurdering. Denne vurdering skal også omfatte enhver påtænkt videreoverførsel.
35. I bør under alle omstændigheder være særligt opmærksomme på alle relevante love, navnlig love, der indeholder krav om videregivelse af personoplysninger til offentlige myndigheder, eller som giver sådanne offentlige myndigheder beføjelse til at tilgå personoplysninger (f.eks. i forbindelse med strafferetshåndhævelse, lovbestemt tilsyn eller formål vedrørende national sikkerhed). Hvis disse krav eller beføjelser begrænser registreredes grundlæggende rettigheder samtidig med, at de respekterer det væsentligste indhold heraf og er nødvendige og forholdsmæssige foranstaltninger i et demokratisk samfund for at beskytte vigtige målsætninger, som det ligeledes er anerkendt i EU-retten eller EU-medlemsstaternes lovgivning⁴⁵, blokerer de muligvis ikke tilsagnene omfattet af det overførselsværktøj, jf. artikel 46 i GDPR, I benytter.

⁴² En overførsel af personoplysninger er en behandlingsaktivitet (artikel 4, nr. 2), i GDPR). Hvis I ønsker at overføre følsomme oplysninger, der er omfattet af artikel 9 og 10 i GDPR, må I kun foretage en overførsel, hvis den er omfattet af en af undtagelserne og betingelserne i artikel 9 og 10 i GDPR og EU-medlemsstaternes lovgivning. I henhold til artikel 32 i GDPR skal I desuden – med importøren som dataansvarlig eller databehandler – gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici for registreredes rettigheder og frihedsrettigheder, der er forbundet med et potentielt brud på persondatasikkerheden i forbindelse med de overførte oplysninger (artikel 4, nr. 12), i GDPR). Kategorierne af overførte oplysninger og deres følsomhed vil være relevante for vurderingen af risikoen og foranstaltningernes hensigtsmæssighed.

⁴³ Nogle tredjelande tillader ikke import af krypterede oplysninger.

⁴⁴ Hvis den dataansvarlige har givet sin forudgående specifikke eller generelle skriftlige godkendelse, jf. artikel 28, stk. 2, i GDPR.

⁴⁵ Jf. artikel 47 og 52 i EU's charter om grundlæggende rettigheder, artikel 23, stk. 1, i GDPR samt Databeskyttelsesrådets henstilling nr. 02/2020 om europæiske væsentlige garantier for

36. I skal vurdere relevante regler og praksis af generel karakter, for så vidt at de kan påvirke effektiv anvendelse af de garantier, som overførselsværktøjet, jf. artikel 46 i GDPR, giver.
37. Forskellige aspekter i det pågældende tredjelandets retssystem, såsom de elementer, der er nævnt i artikel 45, stk. 2, i GDPR, er også relevante ved udførelsen af denne vurdering. F.eks. kan retsstatsforholdene i et tredjeland være relevante ved vurdering af effektiviteten af de mekanismer, enkeltpersoner har til rådighed for (retligt) at kunne klage over ulovlig statslig adgang til personoplysninger. Forekomsten af en omfattende databeskyttelseslovgivning eller en uafhængig databeskyttelsesmyndighed samt tilslutning til internationale instrumenter, der yder databeskyttelsesgarantier, kan bidrage til at sikre, at en stats indgriben er proportional.
38. De forpligtelser eller beføjelser, der følger af en sådan lovgivning eller praksis, vil blive anset for at være i strid med/være uforenelige med tilsagnene i overførselsværktøjet, jf. artikel 46 i GDPR, hvis de⁴⁶:
- ikke respekterer kernen i de grundlæggende rettigheder og frihedsrettighederne i EU's charter om grundlæggende rettigheder eller
 - går videre, end hvad der er nødvendigt og forholdsmæssigt i et demokratisk samfund for at sikre et af de vigtige mål, som det ligeledes er anerkendt i EU-retten eller medlemsstaternes lovgivning, såsom de mål, der er anført i artikel 23, stk. 1, i GDPR.
39. I bør verificere, om dataimportørens tilsagn, der giver registrerede mulighed for at udøve deres rettigheder i henhold til overførselsværktøjet, jf. artikel 46 i GDPR (såsom anmodninger om adgang til, berigtigelse af og sletning af overførte oplysninger samt (retslig) prøvelse), kan håndhæves i praksis, og at tilsagnene ikke hindres af lovgivningen og/eller praksis i bestemmelseslandet.
40. EU-standarder, såsom artikel 47 og 52 i EU's charter om grundlæggende rettigheder, skal anvendes som reference, navnlig for at vurdere, om offentlige myndigheders adgang er begrænset til, hvad der er nødvendigt og forholdsmæssigt i et demokratisk samfund, og om registrerede sikres effektive klagemuligheder.
41. Databeskyttelsesrådets henstilling om europæiske væsentlige garantier⁴⁷ indeholder præciseringer vedrørende de elementer, der skal vurderes for at afgøre, hvorvidt lovgivningen, der regulerer offentlige myndigheders adgang til personoplysninger i et tredjeland, uanset om det er nationale efterretningstjenester eller retshåndhævende myndigheder, kan betragtes som begrundet indgriben⁴⁸. Især dette element bør overvejes grundigt, når den lovgivning, der regulerer offentlige myndigheders adgang til oplysninger, er tvetydig eller ikke er offentligt tilgængelig. Det første krav i de europæiske væsentlige garantier er, at der skal foreligge

overvågningsforanstaltninger af 10. november 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

⁴⁶ Jf. artikel 47 og 52 i EU's charter om grundlæggende rettigheder, artikel 23, stk. 1, i GDPR, C-311/18 (Schrems II), præmis 174 og 187, samt Databeskyttelsesrådets henstilling nr. 02/2020 om europæiske væsentlige garantier for overvågningsforanstaltninger af 10. november 2020.

⁴⁷ EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, 10. november 2020.

⁴⁸ Og derfor ikke som hindring af de tilsagn, der ydes under overførselsværktøjet, jf. artikel 46 i GDPR.

lovgivning, der giver mulighed for denne adgang, når en sådan er påtænkt, og som er offentlig tilgængelig og tilstrækkeligt klar.

42. I forbindelse med dataoverførsler baseret på overførselsværktøjer, jf. artikel 46 i GDPR, kan Databeskyttelsesrådets henstilling om europæiske væsentlige garantier vejlede dataeksportøren ved vurdering af, om sådanne beføjelser er ubegrundet indgriben i dataeksportørens og -importørens forpligtelser til at sikre et beskyttelsesniveau, der i det væsentlige er tilsvarende i henhold til GDPR eller tilsagnene i overførselsværktøjet. Hvis beskyttelsesniveauet i det væsentlige ikke er tilsvarende, vil det navnlig være tydeligt, hvis lovgivningen og/eller praksis i tredjelandet, der er relevant for jeres overførsel, ikke opfylder kravene i de europæiske væsentlige garantier. Det Europæiske Databeskyttelsesråd gentager, at de europæiske væsentlige garantier er en referencestandard til vurdering af et indgreb, der er foretaget under et tredjelands overvågningsforanstaltninger i forbindelse med internationale dataoverførsler. Disse standarder udspringer af EU-retten samt retspraksis fra EU-Domstolen og EMD, som er bindende for EU-medlemsstater.
43. Jeres vurdering skal først og fremmest være baseret på den offentligt tilgængelige lovgivning. En undersøgelse af tredjelandets offentlige myndigheders praksis vil ligeledes gøre det muligt for jer at verificere, om garantierne i overførselsværktøjet, jf. artikel 46 i GDPR, i praksis kan være et tilstrækkeligt middel til at sikre en effektiv beskyttelse af de overførte personoplysninger.⁴⁹ En undersøgelse af gældende praksis i tredjelandet vil navnlig være vigtig for jeres vurdering i de nedenfor beskrevne situationer.
- 43.1 **Relevant lovgivning i tredjelandet kan formelt opfylde EU's standarder vedrørende grundlæggende rettigheder og frihedsrettigheder og nødvendigheden og proportionaliteten af begrænsninger heraf.** Dets offentlige myndigheders praksis (f.eks. adgang til personoplysninger, der er i den private sektors besiddelse, eller når de håndhæver – eller ikke håndhæver – lovgivning som tilsynsmyndigheder eller retlige myndigheder) kan imidlertid klart være et udtryk for, at de ikke normalt anvender/overholder den lovgivning, der i princippet regulerer deres aktiviteter. I dette tilfælde skal I tage hensyn til denne praksis i jeres vurdering og tage i betragtning, at overførselsværktøjet, jf. artikel 46 i GDPR, ikke i sig selv (dvs. uden supplerende foranstaltninger) effektivt kan sikre et beskyttelsesniveau, der i det væsentlige er tilsvarende. I så fald skal I, hvis I ønsker at gå videre med overførslen, gennemføre passende supplerende foranstaltninger.
- 43.2 **Relevant lovgivning i tredjelandet (f.eks. om adgang til personoplysninger, der er i den private sektors besiddelse) er eventuelt mangelfuld.** I dette tilfælde kan I ikke automatisk udlede af denne mangel på relevant lovgivning, at jeres overførselsværktøj, jf. artikel 46 i GDPR, kan anvendes effektivt. I skal kontrollere, om der er indikatorer for gældende praksis i landet, som er uforenelig med EU-retten og tilsagnene i overførselsværktøjet, jf. artikel 46 i GDPR. Hvis der foreligger uforenelig praksis, kan overførselsværktøjet, jf. artikel 46 i GDPR, ikke i sig selv (dvs. uden supplerende foranstaltninger) effektivt sikre et beskyttelsesniveau, der i det væsentlige er tilsvarende. I så fald skal I, hvis I ønsker at gå videre med overførslen, gennemføre passende supplerende foranstaltninger.

⁴⁹ C-311/18 (Schrems II), præmis 126.

43.3 Vurderingen kan vise, at den relevante lovgivning i tredjelandet kan være problematisk⁵⁰, og at de overførte oplysninger og/eller den pågældende importør er eller kan være omfattet af anvendelsesområdet for denne problematiske lovgivning.⁵¹

I lyset af usikkerheden med hensyn til en eventuel anvendelse af problematisk lovgivning på jeres overførsel kan I beslutte at:

- suspendere overførslen
- gennemføre supplerende foranstaltninger⁵² for at forebygge risikoen for en eventuel anvendelse på jeres importør og/eller jeres overførte oplysninger af lovgivning og/eller praksis i dataimportørens tredjeland, som kan bringe overførselsværktøjets kontraktlige garanti for et beskyttelsesniveau, der i det væsentlige svarer til det niveau, der er sikret i EØS, i fare, eller
- alternativt kan I beslutte at gå videre med overførslen uden at skulle gennemføre supplerende foranstaltninger, hvis I vurderer, at I ikke har nogen grund til at tro, at den relevante og problematiske lovgivning i praksis vil blive anvendt på jeres overførte oplysninger og/eller importør. I skal via jeres vurdering have påvist og dokumenteret, hvor det er relevant i samarbejde med importøren, at lovgivningen ikke fortolkes og/eller i praksis anvendes på jeres overførte oplysninger og importør, også under hensyntagen til erfaringerne blandt andre aktører inden for samme sektor og/eller i forbindelse med lignende overførte personoplysninger og de yderligere informationskilder, der er beskrevet nedenfor.⁵³

I skal derfor have påvist og dokumenteret med en detaljeret rapport⁵⁴, at problematisk lovgivning ikke i praksis vil blive anvendt på jeres overførte oplysninger og/eller importør, og at det derfor ikke vil forhindre importøren i at opfylde sine forpligtelser i henhold til overførselsværktøjet, jf. artikel 46 i GDPR.⁵⁵

⁵⁰ Ved "problematiske lovgivning" forstås lovgivning, som 1) pålægger modtageren af personoplysninger fra Den Europæiske Union forpligtelser og/eller påvirker de overførte oplysninger på en måde, der kan bringe overførselsværktøjets kontraktlige garanti for et i det væsentlige tilsvarende beskyttelsesniveau i fare, og 2) ikke respekterer kernen i de grundlæggende rettigheder og frihedsrettighederne, der er anerkendt i EU's charter om grundlæggende rettigheder, eller går videre, end hvad der er nødvendigt og forholdsmæssigt i et demokratisk samfund for at sikre et af de vigtige mål, som det ligeledes er anerkendt i EU-retten eller EU-medlemsstaternes lovgivning, såsom de mål, der er anført i artikel 23, stk. 1, i GDPR.

⁵¹ Det kan være uklart, om importøren og/eller de overførte oplysninger er omfattet af anvendelsesområdet for de generelle udtryk, der ofte anvendes i den nationale sikkerhedslovgivning for at begrænse deres anvendelsesområde, såsom eksempelvis "udbydere af elektroniske kommunikationstjenester" og "udenlandske efterretningsoplysninger".

⁵² Jf. betragtning 109 i GDPR og C-311/18 (Schrems II), præmis 132.

⁵³ Jf. punkt 45-47.

⁵⁴ I de rapporter, I udarbejder, skal indgå omfattende oplysninger om den juridiske vurdering af lovgivningen og praksis og anvendelsen heraf på de konkrete overførsler, den interne procedure til udarbejdelse af vurderingen (herunder oplysninger om aktører involveret i vurderingen, f.eks. advokatfirmaer, konsulenter eller interne afdelinger) og datoer for kontrollen. Rapporterne skal godkendes af eksportørens retlige repræsentant.

⁵⁵ Påvisning af, at problematisk lovgivning ikke i praksis anvendes på jeres overførte oplysninger og importør, også under hensyntagen til erfaringerne blandt andre aktører inden for samme sektor og/eller i forbindelse med lignende overførte personoplysninger, fritager jer ikke fra at træffe de nødvendige supplerende foranstaltninger

Mulige informationskilder

44. Jeres dataimportør bør give jer de relevante kilder og oplysninger om det tredjeland, hvor denne er etableret, samt den lovgivning og gældende praksis, der finder anvendelse på overførslen.
45. I og jeres importør kan fuldende vurderingen med oplysninger indhentet fra kilder, såsom dem, der er anført som eksempler i bilag 3.
46. Ud over tredjelandets lovgivning, som er gældende for overførslen, bør kilder og oplysninger være relevante, objektive, pålidelige, verificerbare og offentligt tilgængelige eller på anden måde tilgængelige for at afgøre, om jeres overførselsværktøj, jf. artikel 46 i GDPR, kan anvendes effektivt⁵⁶, og I skal vurdere og dokumentere dette.

Relevant: Oplysningerne skal være relevante for den konkrete overførsel og/eller importør og overholde kravene i henhold til EU-retten og overførselsværktøjet, jf. artikel 46 i GDPR, og ikke alt for generelle eller abstrakte.

Objektive oplysninger: Oplysninger, der understøttes af empirisk evidens baseret på viden erhvervet tidligere, ikke antagelser om potentielle begivenheder og risici.

Pålidelig: Eksportøren og importøren skal objektivt vurdere informationskildernes og selve oplysningernes pålidelighed og evaluere dem særskilt.

Verificerbar: Oplysninger og konklusioner skal være verificerbare eller kunne modstilles med andre typer af informationskilder som en del af en samlet vurdering, også for at gøre det muligt for den kompetente tilsynsmyndighed eller retlige myndighed om nødvendigt at kontrollere, om disse oplysninger er objektive og pålidelige.

Offentligt tilgængelige eller på anden måde tilgængelige oplysninger: Oplysningerne bør fortrinsvis være offentlige eller i det mindste tilgængelige for at lette verifikationen af ovenstående kriterier og sikre, at de kan deles med tilsynsmyndigheder, retlige myndigheder og i sidste ende registrerede.

47. I kan desuden tage importørens dokumenterede praktiske erfaringer med relevante tidligere tilfælde af anmodninger om adgang modtaget fra offentlige myndigheder i tredjelandet i betragtning. I kan kun udnytte importørens erfaringer som en yderligere informationskilde, hvis tredjelandets lovgivning ikke forbyder importøren at give oplysninger om anmodninger om offentliggørelse fra offentlige myndigheder eller fraværet af sådanne anmodninger (og I bør også dokumentere en sådan vurdering). I skal imidlertid bemærke, at den omstændighed, at der ikke foreligger tidligere tilfælde af anmodninger modtaget af importøren, aldrig i sig selv kan betragtes som en afgørende faktor med hensyn til effektiviteten af overførselsværktøjet, jf. artikel 46 i

for at beskytte personoplysninger i forbindelse med overførslen og behandlingen heraf i bestemmelseslandet (f.eks. ende-til-ende-kryptering af data – se eksempler på tekniske supplerende foranstaltninger i bilag 2), hvis jeres analyse af den gældende lovgivning i bestemmelseslandet viser, at adgang til oplysninger også kan finde sted, selv uden importørens indgriben, på dette tidspunkt af overførslen. I har måske allerede gennemført sådanne foranstaltninger med importøren som dataansvarlig eller databehandler i henhold til artikel 32 i GDPR.
⁵⁶ Der henvises til bilag 3 for en ikke-udtømmende liste over informationskilder, som I og importøren kan benytte.

GDPR, som gør det muligt at gå videre med overførslen uden supplerende foranstaltninger. I kan tage disse oplysninger i betragtning, sammen med andre typer af oplysninger indhentet fra andre kilder, som en del af jeres samlede vurdering af lovgivningen og praksis i tredjelandet i relation til jeres overførsel. Importørens relevante og dokumenterede erfaringer bør underbygges og ikke modsiges af andre relevante, objektive, pålidelige, verificerbare og offentligt tilgængelige eller på anden måde tilgængelige oplysninger om den praktiske anvendelse af den relevante lovgivning (f.eks. forekomsten eller fraværet af anmodninger om adgang modtaget af andre aktører inden for samme sektor og/eller i forbindelse med lignende overførte personoplysninger⁵⁷ og/eller anvendelsen af lovgivningen i praksis, såsom retspraksis og rapporter fra uafhængige tilsynsorganer).

Resultater af jeres vurdering

48. Denne samlede vurdering af den lovgivning og praksis i jeres importørs tredjeland, som er gældende for jeres overførsel, bør udføres med fornøden omhu og dokumenteres grundigt. Jeres kompetente tilsynsmyndighed og/eller retlige myndighed kan anmode herom og drage jer til ansvar for enhver beslutning, I træffer på dette grundlag.⁵⁸
49. Jeres vurdering kan i sidste ende vise, at det overførselsværktøj, jf. artikel 46 i GDPR, som I benytter, enten:
- effektivt sikrer, at de overførte personoplysninger sikres et beskyttelsesniveau i tredjelandet, der i det væsentlige svarer til det niveau, der er sikret i EØS. Tredjelandets lovgivning og praksis, som er gældende for overførslen, giver dataimportøren mulighed for at opfylde sine forpligtelser i overensstemmelse med det valgte overførselsværktøj. I bør foretage vurderingen igen med passende mellemrum, eller når der forekommer betydelige ændringer (se trin 6), eller
 - ikke effektivt sikrer et beskyttelsesniveau, der i det væsentlige er tilsvarende. Dataimportøren kan ikke opfylde sine forpligtelser som følge af tredjelandets lovgivning og/eller praksis, som er gældende for overførslen, og som ikke opfylder EU's standarder vedrørende grundlæggende rettigheder og frihedsrettigheder og nødvendigheden og proportionaliteten af begrænsninger heraf for at beskytte legitime mål af almen interesse. EU-Domstolen understregede, at hvis overførselsværktøjet, jf. artikel 46 i GDPR, viser sig at være mangelfuldt, er det dataeksportørens ansvar enten at træffe effektive supplerende foranstaltninger eller ikke at overføre personoplysningerne.⁵⁹

Eksempel:

Baggrund:

⁵⁷ Erfaringerne kunne være andre enheders erfaringer, som I har direkte kendskab til på grund af tidligere overførsler af samme art, som I har foretaget, eller som fremgår af relevant retspraksis, rapporter fra NGO'er osv. (se bilag 3).

⁵⁸ Artikel 5, stk. 2, i GDPR.

⁵⁹ EU-Domstolen, C-311/18 (Schrems II), præmis 134 og 135.

EU-Domstolen fastslog, at section 702 i USA's FISA (Foreign Intelligence Surveillance Act) ikke overholder de mindstekrav, der følger af proportionalitetsprincippet i EU-retten, og derfor ikke kan anses for at være begrænset til det strengt nødvendige. Det betyder, at beskyttelsesniveauet i de programmer, der er godkendt i medfør af section 702 i FISA, ikke i det væsentlige svarer til de garantier, der kræves i EU-retten.

Vurdering:

Hvis I på grundlag af jeres vurdering af den relevante amerikanske lovgivning vurderer, at jeres overførsel kunne være omfattet af anvendelsesområdet for section 702 i FISA, men I er usikre på, om den er omfattet af dens praktiske anvendelsesområde, kan I beslutte enten at:

1. indstille overførslen
2. vedtage passende supplerende foranstaltninger, der effektivt sikrer et niveau for beskyttelse af de overførte oplysninger, der i det væsentlige svarer til det, der er sikret i EØS, eller
3. se nærmere på andre objektive, pålidelige, relevante, verificerbare og fortrinsvis offentligt tilgængelige oplysninger (som kan omfatte oplysninger, som jeres dataimportør giver jer) for at klarlægge anvendelsesområdet i praksis af section 702 i FISA med hensyn til jeres konkrete overførsel. Disse oplysninger bør give svar på en række relevante spørgsmål, såsom følgende:

- Viser offentligt tilgængelige oplysninger, at der foreligger et retligt forbud mod at give oplysninger om en specifik anmodning om adgang til oplysninger, der er modtaget, og omfattende begrænsninger med hensyn til at give generelle oplysninger om modtagne anmodninger om adgang til oplysninger eller fraværet af modtagne anmodninger?

- Har jeres dataimportør bekræftet at have modtaget anmodninger om adgang til oplysninger fra amerikanske offentlige myndigheder tidligere? Eller har jeres dataimportør bekræftet ikke at have modtaget anmodninger om adgang til oplysninger fra amerikanske offentlige myndigheder tidligere eller ikke at være afskåret fra at give oplysninger om sådanne anmodninger eller fraværet heraf?

- Viser offentligt tilgængelige oplysninger, som I har indhenter vedrørende amerikansk retspraksis og rapporter fra tilsynsorganer, civilsamfundsorganisationer og akademiske institutioner⁶⁰, at dataimportører fra den samme sektor som jeres importør har modtaget anmodninger om adgang til oplysninger i forbindelse med lignende overførte oplysninger tidligere?

På grundlag af de svar på disse spørgsmål, som I får i forbindelse med den samlede vurdering, konkluderer I, at:

- section 702 i FISA i praksis finder anvendelse på jeres konkrete overførsel og derfor bringer effektiviteten af jeres overførselsværktøj, jf. artikel 46 i GDPR, i fare. Hvis I ønsker at gå videre med overførslen, skal I derfor overveje, hvor det er relevant i samarbejde med importøren, om I kan vedtage supplerende foranstaltninger, der effektivt sikrer et niveau for beskyttelse af de overførte oplysninger, der i det væsentlige svarer til det, der er sikret i EØS. Hvis I ikke kan finde effektive supplerende foranstaltninger, må I ikke overføre personoplysningerne eller

⁶⁰ F.eks. bestemmelser i section 702 i FISA, procesreglementet for Foreign Intelligence Surveillance Court (FISC), afklassificerede udtalelser og afgørelser fra FISC, praksis fra amerikanske domstole, rapporter og protokollater fra Privacy and Civil Liberties Oversight Board (PCLOB), rapporter fra Office of the Inspector General – det amerikanske justitsministerium, rapporter fra NSA Director of Civil Liberties and Privacy Office, rapporter udarbejdet af Congressional Research Service, rapporter fra American Civil Liberties Union Foundation (ACLU).

- section 702 i FISA finder ikke i praksis anvendelse på jeres konkrete overførsel og bringer derfor ikke effektiviteten af jeres overførselsværktøj, jf. artikel 46 i GDPR, i fare. I kan derefter gå videre med overførslen uden supplerende foranstaltninger.

2.4 Trin 4: Vedtag supplerende foranstaltninger

50. Hvis jeres evaluering under trin 3 har vist, at jeres overførselsværktøj, jf. artikel 46 i GDPR, ikke er effektivt, skal I, hvor det er relevant i samarbejde med importøren, overveje, om der er supplerende foranstaltninger, som sammen med garantierne i overførselsværktøjer kan sikre, at de overførte oplysninger i tredjelandet sikres et beskyttelsesniveau, der i det væsentlige svarer til den beskyttelse, der er sikret i EU.⁶¹ "Supplerende foranstaltninger" er pr. definition et supplement til garantierne ved overførselsværktøjet, jf. artikel 46 i GDPR, og til alle andre gældende sikkerhedskrav (f.eks. tekniske sikkerhedsforanstaltninger), der er fastsat i GDPR.⁶²
51. I skal i hvert enkelt tilfælde fastlægge, hvilke supplerende foranstaltninger der vil være effektive for en række overførsler til et bestemt tredjeland, når der benyttes et overførselsværktøj, jf. artikel 46 i GDPR. I behøver ikke at gentage vurderingen hver gang, I foretager den samme overførsel af en specifik type oplysninger til det samme tredjeland. Nogle af de oplysninger, der er planlagt til overførsel, kan kræve supplerende foranstaltninger, mens det i givet fald ikke er tilfældet med hensyn til andre oplysninger (på baggrund af den formelle og/eller praktiske anvendelse af tredjelandets lovgivning). I kan arbejde videre på de tidligere vurderinger og konklusioner under trin 1, 2 og 3 herover og sammenholde de supplerende foranstaltningers potentielle virkning med disse vurderinger, for så vidt angår garantien for det krævede beskyttelsesniveau.
52. Supplerende foranstaltninger kan som udgangspunkt være af kontraktlig, teknisk eller organisatorisk art. Ved at kombinere forskellige foranstaltninger på en måde, der understøtter og bygger videre på hinanden, kan de forstærke beskyttelsesniveauet og således bidrage til at leve op til EU's standarder.
53. Kontraktlige og organisatoriske foranstaltninger alene vil generelt ikke overvinde tredjelandets offentlige myndigheders adgang til personoplysninger på grundlag af problematisk lovgivning og/eller praksis.⁶³ Der vil være situationer, hvor kun korrekt gennemførte tekniske

⁶¹ C-311/18 (Schrems II), præmis 96.

⁶² Betragtning 109 i GDPR og C-311/18 (Schrems II), præmis 133.

⁶³ Ved "problematiske lovgivning" forstås lovgivning, som 1) pålægger modtageren af personoplysninger fra Den Europæiske Union forpligtelser og/eller påvirker de overførte oplysninger på en måde, der kan bringe overførselsværktøjets kontraktlige garanti for et i det væsentlige tilsvarende beskyttelsesniveau i fare, og 2) ikke respekterer kernen i de grundlæggende rettigheder og frihedsrettighederne, der er anerkendt i EU's charter om grundlæggende rettigheder, eller går videre, end hvad der er nødvendigt og forholdsmæssigt i et demokratisk samfund for at sikre et af de vigtige mål, som det ligeledes er anerkendt i EU-retten eller EU-medlemsstaternes lovgivning, såsom de mål, der er anført i artikel 23, stk. 1, i GDPR.

foranstaltninger vil kunne forhindre eller gøre offentlige myndigheder i tredjelandes adgang til personoplysninger ineffektiv, navnlig i forbindelse med overvågning.⁶⁴ I disse situationer kan kontraktlige eller organisatoriske foranstaltninger supplere tekniske foranstaltninger og styrke oplysningernes samlede beskyttelsesniveau (f.eks. ved at indføre kontrol og eliminere automatik med hensyn til forsøg fra offentlige myndigheders side på at opnå adgang til oplysninger på en måde, der ikke er i overensstemmelse med EU's standarder.

54. I kan, hvor det er relevant i samarbejde med dataimportøren, se på følgende (ikke-udtømmende) optegnelse over faktorer, der kan bidrage til at fastlægge, hvilke supplerende foranstaltninger der vil være mest effektive til at beskytte de overførte oplysninger mod offentlige myndigheders anmodninger om adgang til oplysninger på grundlag af problematisk lovgivning, der anvendes i praksis:

- format af oplysninger, der skal overføres (f.eks. almindelig tekst/pseudonymiseret eller krypteret)
- arten af oplysninger (f.eks. sikres kategorier af oplysninger, der er omfattet af artikel 9 og 10 i GDPR, et højere beskyttelsesniveau i EØS)⁶⁵
- længde og kompleksitet af arbejdsgangen vedrørende databehandlingen, antal aktører involveret i behandlingen og forholdet mellem dem (omfatter overførslerne f.eks. flere dataansvarlige eller både dataansvarlige og databehandlere eller inddragelse af databehandlere, der overfører oplysningerne fra jer til jeres dataimportør – under hensyntagen til de relevante bestemmelser, som er gældende for overførslerne, i henhold til bestemmelseslandets lovgivning)⁶⁶
- teknik eller parametre for den praktiske anvendelse af tredjelandets lovgivning konkluderet i trin 3
- mulighed for, at oplysningerne kan være genstand for videreoverførsel inden for samme tredjeland eller endda til andre tredjelande (f.eks. ved at benytte dataimportørens underdatabehandlere⁶⁷).

⁶⁴ Når en sådan adgang går videre, end hvad der er nødvendigt og forholdsmæssigt i et demokratisk samfund, jf. artikel 47 og 52 i EU's charter om grundlæggende rettigheder, artikel 23, stk. 1, i GDPR samt Databeskyttelsesrådets henstilling nr. 02/2020 om europæiske væsentlige garantier for overvågningsforanstaltninger af 10. november 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

⁶⁵ Se fodnote 42.

⁶⁶ GDPR pålægger dataansvarlige og databehandlere forskellige forpligtelser. Overførsler kan være dataansvarlig-til-dataansvarlig, mellem fælles dataansvarlige, dataansvarlig-til-databehandler og, med forbehold af den dataansvarliges tilladelse, databehandler-til-dataansvarlig eller databehandler-til-databehandler.

⁶⁷ Se fodnote 26.

Eksempler på supplerende foranstaltninger

55. Nogle eksempler på tekniske, kontraktlige og organisatoriske foranstaltninger, der kunne overvejes, hvis de ikke allerede indgår i det benyttede overførselsværktøj, jf. artikel 46 i GDPR, fremgår af de ikke-udtømmende lister, der er beskrevet i bilag 2.

56. Hvis I har indført effektive supplerende foranstaltninger, der i kombination med det valgte overførselsværktøj, jf. artikel 46 i GDPR, giver et beskyttelsesniveau, der nu i det væsentlige svarer til det beskyttelsesniveau, der sikres i EØS, kan I gå videre med overførslerne.

57. Hvis I ikke kunne finde eller implementere effektive supplerende foranstaltninger, der sikrer, at de overførte personoplysninger har et beskyttelsesniveau, der i det væsentlige svarer til det i EU⁶⁸, må I ikke begynde at overføre personoplysninger til det pågældende tredjeland på baggrund af det overførselsværktøj, jf. artikel 46 i GDPR, I benytter. Hvis I allerede foretager overførsler, skal I suspendere eller indstille overførslen af personoplysninger.⁶⁹ I henhold til garantierne i det overførselsværktøj, jf. artikel 46 i GDPR, I benytter, bør de oplysninger, I allerede har overført til det pågældende tredjeland, samt kopier af dem, returneres til jer eller fuldstændigt destrueres af importøren.⁷⁰

Eksempel:

Lovgivningen i tredjelandet forbyder de supplerende foranstaltninger, I har udpeget (f.eks. forbud mod brug af kryptering), eller forhindrer på anden måde, at de er effektive. I må ikke begynde overførsel af personoplysninger til dette land, eller I skal indstille igangværende eksisterende overførsler til landet.

58. Den kompetente tilsynsmyndighed kan pålægge enhver anden afhjælpende foranstaltning (f.eks. en bøde), hvis I, til trods for at I ikke kan påvise et beskyttelsesniveau i tredjelandet, der i det væsentlige svarer til niveauet i EU, påbegynder eller fortsætter med overførslen.

⁶⁸ Når en sådan adgang går videre, end hvad der er nødvendigt og forholdsmæssigt i et demokratisk samfund, jf. artikel 47 og 52 i EU's charter om grundlæggende rettigheder, artikel 23, stk. 1, i GDPR samt Databeskyttelsesrådets henstilling nr. 02/2020 om europæiske væsentlige garantier for overvågningsforanstaltninger af 10. november 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

⁶⁹ C-311/18 (Schrems II), præmis 135.

⁷⁰ Jf. eksempelvis klausul 12 i bilaget til afgørelse 87/2010 om standardkontraktbestemmelser, jf. den (valgfrie) supplerende bestemmelse om ophør i bilag B til beslutning 2004/915/EF om standardkontraktbestemmelser.

2.5 Trin 5: Proceduremæssige trin, hvis I har fastlagt effektive supplerende foranstaltninger

59. De proceduremæssige trin, I eventuelt skal tage, hvis I har fastlagt effektive supplerende foranstaltninger, der skal indføres, kan være forskellige afhængigt af det overførselsværktøj, jf. artikel 46 i GDPR, I benytter eller har planlagt at benytte.

2.5.1 Standardbestemmelser om databeskyttelse (artikel 46, stk. 2, litra c) og d), i GDPR)

60. Når I påtænker at indføre supplerende foranstaltninger i tillæg til standardbestemmelser om databeskyttelse, behøver I ikke anmode om tilladelse fra den kompetente tilsynsmyndighed for at tilføje denne type kontraktbestemmelser eller yderligere garantier, såfremt de fastlagte supplerende foranstaltninger ikke direkte eller indirekte er i strid med standardbestemmelserne om databeskyttelse og er tilstrækkelige til at sikre, at det beskyttelsesniveau, der er sikret ved GDPR, ikke undermineres.⁷¹ Dataeksportøren og -importøren skal sikre, at de yderligere bestemmelser ikke kan fortolkes på en måde, der begrænser rettighederne og forpligtelserne i standardbestemmelserne om databeskyttelse eller på anden måde begrænser databeskyttelsesniveauet. Dette, herunder alle bestemmelsers utvetydighed, bør I kunne påvise i henhold til ansvarlighedsprincippet og jeres pligt til at yde et tilstrækkeligt databeskyttelsesniveau. De kompetente tilsynsmyndigheder har bemyndigelse til at revidere disse supplerende bestemmelser, hvis det er nødvendigt (f.eks. hvis der er en klage eller en undersøgelse på eget initiativ).
61. Hvis I ønsker at ændre selve standardbestemmelserne om databeskyttelse, eller hvis de tilføjede supplerende foranstaltninger direkte eller indirekte er i modstrid med standardbestemmelserne om databeskyttelse, anses I ikke længere for at henholde jer til standardkontraktbestemmelser⁷² og skal ansøge om tilladelse hos den kompetente tilsynsmyndighed i overensstemmelse med artikel 46, stk. 3, litra a), i GDPR.

⁷¹ Betragtning 109 i GDPR fastslår: "Den dataansvarliges eller databehandlerens mulighed for at bruge standardbestemmelser om databeskyttelse vedtaget af Kommissionen eller en tilsynsmyndighed bør hverken udelukke muligheden for, at den dataansvarlige eller databehandleren medtager standardbestemmelser om databeskyttelse i en bredere kontrakt, såsom en kontrakt mellem databehandleren og en anden databehandler, eller medtager andre bestemmelser eller yderligere garantier, såfremt de hverken direkte eller indirekte er i strid med de standardkontraktbestemmelser, der er vedtaget af Kommissionen eller en tilsynsmyndighed, eller berører de registreredes grundlæggende rettigheder eller frihedsrettigheder.". Der er lignende bestemmelser i de sæt standardbestemmelser om databeskyttelse, som Europa-Kommissionen har vedtaget i medfør af direktiv 95/45/EF.

⁷² Se analogt Databeskyttelsesrådets udtalelse 17/2020 om udkast til standardkontraktbestemmelser forelagt af den slovenske tilsynsmyndighed (artikel 28, stk. 8, i GDPR) om artikel 28-standardbestemmelser om databeskyttelse, der allerede er vedtaget og indeholder en lignende bestemmelse ("Desuden minder Databeskyttelsesrådet om, at muligheden for at bruge standardkontraktbestemmelser, der er vedtaget af en tilsynsmyndighed, ikke udelukker muligheden for, at parterne medtager andre bestemmelser eller yderligere garantier, såfremt de hverken direkte eller indirekte er i strid med de standardkontraktbestemmelser, der er vedtaget, eller berører de registreredes grundlæggende rettigheder eller frihedsrettigheder. Såfremt standardkontraktbestemmelserne ændres, vil parterne endvidere ikke længere kunne anses for at have gennemført vedtagne standardkontraktbestemmelser"), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202017_art28sccs_si_en.pdf.

2.5.2 Bindende virksomhedsregler (artikel 46, stk. 2, i GDPR)

62. Begrundelsen, der blev fremført i Schrems II-dommen, finder også anvendelse på andre overførselsinstrumenter i henhold til artikel 46, stk. 2, i GDPR, fordi alle disse instrumenter er grundlæggende af kontraktlig art, dvs. at garantierne i disse instrumenter og parternes tilsagn under instrumenterne ikke kan binde offentlige myndigheder i et tredjeland.⁷³
63. Schrems II-dommen er relevant for overførsler af personoplysninger på baggrund af bindende virksomhedsregler, eftersom lovgivning i tredjelände kan påvirke den beskyttelse, sådanne instrumenter giver.
64. Alle tilsagn, der skal medtages, vil fremgå af de ajourførte referencer til WP256/257⁷⁴, hvortil alle grupper, der benytter bindende virksomhedsregler som overførselsværktøjer, skal tilpasse deres eksisterende og fremtidige bindende virksomhedsregler.
65. Domstolen fremhævede, at det er dataeksportørens og dataimportørens ansvar at vurdere, om det beskyttelsesniveau, der kræves i EU-retten, respekteres i det pågældende tredjeland, med henblik på at fastslå, om garantierne i standardkontraktbestemmelserne eller de bindende virksomhedsregler kan overholdes i praksis. Hvis dette ikke er tilfældet, bør I vurdere, om I kan iværksætte supplerende foranstaltninger for at sikre et beskyttelsesniveau, der i det væsentlige svarer til niveauet i EØS, og om lovgivningen og praksis i tredjelandet vil kollidere med disse supplerende foranstaltninger og dermed underminere deres virkning.

2.5.3 Ad hoc-kontraktbestemmelser (artikel 46, stk. 3, litra a), i GDPR)

66. Begrundelsen, der blev fremført i Schrems II-dommen, finder også anvendelse på andre overførselsinstrumenter i henhold til artikel 46, stk. 2, i GDPR, fordi alle disse instrumenter grundlæggende er af kontraktlig art, dvs. at garantierne i disse instrumenter og parternes tilsagn under instrumenterne ikke kan binde offentlige myndigheder i et tredjeland.⁷⁵ Schrems II-dommen er derfor relevant for overførsler af personoplysninger på baggrund af ad hoc-kontraktbestemmelser, eftersom lovgivningen i tredjelände kan påvirke den beskyttelse, sådanne instrumenter giver.

2.6 Trin 6: Gentag evalueringen med passende mellemrum

67. I skal løbende, og hvor det er relevant i samarbejde med dataimportører, overvåge udviklingen i det tredjeland, I har overført personoplysninger til, som kan påvirke jeres oprindelige vurdering af beskyttelsesniveauet og de beslutninger, I eventuelt har truffet på dette grundlag vedrørende jeres overførsler. Ansvarlighed er en løbende forpligtelse (artikel 5, stk. 2, i GDPR).
68. I bør have indført tilstrækkeligt gode mekanismer til at sikre, at I straks suspenderer eller indstiller overførsler, hvis:

⁷³ EU-Domstolen, C-311/18 (Schrems II), præmis 132.

⁷⁴ Artikel 29-Gruppens arbejdsdokument indeholder en tabel med de elementer og principper, der forekommer i bindende virksomhedsregler, senest revideret og vedtaget den 6. februar 2018, WP 256 rev.01; Artikel 29-Gruppens arbejdsdokument indeholder en tabel med de elementer og principper, der forekommer i bindende virksomhedsregler, senest revideret og vedtaget den 6. februar 2018, WP 257 rev.01.

⁷⁵ EU-Domstolen, C-311/18 (Schrems II), præmis 132.

- importøren har overtrådt eller ikke kan efterkomme de tilsagn, denne har givet under overførselsværktøjet, jf. artikel 46 i GDPR, eller
- de supplerende foranstaltninger ikke længere er effektive i det pågældende tredjeland.

3 KONKLUSION

69. GDPR fastlægger regler om behandling af personoplysninger i EØS og tillader derved fri udveksling af personoplysninger inden for EØS. Kapitel V i GDPR regulerer overførsler af personoplysninger til tredjelande og sætter baren højt: overførslen må ikke underminere det beskyttelsesniveau, fysiske personer er sikret ved GDPR (artikel 44 i GDPR). EU-Domstolen understreger i sin dom i sag C-311/18 (Schrems II) behovet for at sikre opretholdelse af det beskyttelsesniveau, der er sikret ved GDPR, for personoplysninger, der overføres til et tredjeland.⁷⁶
70. For at sikre et beskyttelsesniveau, der i det væsentlige er tilsvarende, skal I først og fremmest kende jeres overførsler. I skal også verificere, om de oplysninger, I overfører, er tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles.
71. I skal desuden fastlægge det overførselsværktøj, I benytter til jeres overførsler. Hvis overførselsværktøjet ikke er en afgørelse om tilstrækkelighed, skal I for hvert enkelt tilfælde afgøre, om lovgivningen eller praksis i destinationslandet underminerer de garantier, som overførselsværktøjet, jf. artikel 46 i GDPR, giver i forbindelse med jeres overførsler. Hvis overførselsværktøjet, jf. artikel 46 i GDPR, alene ikke kan sikre de personoplysninger, I overfører, et beskyttelsesniveau, der i det væsentlige svarer til det i EØS, skal supplerende foranstaltninger udbedre manglen.
72. Hvis I ikke kunne finde eller implementere effektive supplerende foranstaltninger, der sikrer, at de overførte personoplysninger har et beskyttelsesniveau, der i det væsentlige svarer til det i EØS, må I ikke begynde at overføre personoplysninger til det pågældende tredjeland på baggrund af det overførselsværktøj, I har valgt. Hvis I allerede foretager overførsler, skal I straks suspendere eller indstille overførslen af personoplysninger.
73. Den kompetente tilsynsmyndighed har bemyndigelse til at suspendere eller indstille overførsler af personoplysninger til tredjelandet, hvis de overførte data ikke sikres den beskyttelse, der kræves i EU-retten, særlig artikel 45 og 46 i GDPR og chartret om grundlæggende rettigheder.

For Det Europæiske Databeskyttelsesråd —

Formanden

(Andrea Jelinek)

⁷⁶ C-311/18 (Schrems II), præmis 93.

BILAG 1: DEFINITIONER

- "Tredjeland" betyder et land, som ikke er en EØS-medlemsstat.
- "EØS" betyder Det Europæiske Økonomiske Samarbejdsområde, og det omfatter EU's medlemsstater og Island, Norge og Liechtenstein. GDPR finder anvendelse for sidstnævnte som følge af EØS-aftalen, navnlig dennes bilag XI og protokol 37.
- "GDPR" henviser til Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse).
- "Chartret" henviser til Den Europæiske Unions charter om grundlæggende rettigheder, EUT C 326 af 26.10.2012, s. 391-407.
- "EU-Domstolen" eller "Domstolen" henviser til Den Europæiske Unions Domstol. Den udgør Den Europæiske Unions retlige myndighed, og i samarbejde med medlemsstaternes domstole og domsmyndigheder sikrer den en ensartet anvendelse og fortolkning af EU-retten.
- "Dataeksportør" betyder den dataansvarlige eller databehandleren inden for EØS, som overfører personoplysninger til en dataansvarlig eller databehandler i et tredjeland.
- "Dataimportør" betyder den dataansvarlige eller databehandleren i et tredjeland, som modtager eller får adgang til personoplysninger, der er overført fra EØS.
- "Overførselsværktøj, jf. artikel 46 i GDPR", henviser til de fornødne garantier under artikel 46 i GDPR, som dataeksportører skal fastlægge ved overførsel af personoplysninger til et tredjeland, når der mangler en afgørelse om tilstrækkelighed i henhold til artikel 45, stk. 3, i GDPR. Artikel 46, stk. 2 og 3, i GDPR indeholder listen over overførselsværktøjer, jf. artikel 46 i GDPR, som dataansvarlige og databehandlere kan benytte.
- "Standardkontraktbestemmelser" betyder standardbestemmelser om databeskyttelse, der er vedtaget af Europa-Kommissionen til overførsler af personoplysninger mellem dataansvarlige og databehandlere i EØS og dataansvarlige eller databehandlere uden for EØS. Standardkontraktbestemmelser vedtaget af Europa-Kommissionen er et overførselsværktøj under GDPR i medfør af artikel 46, stk. 2, litra c), og artikel 46, stk. 5, i GDPR.

BILAG 2: EKSEMPLER PÅ SUPPLERENDE FORANSTALTNINGER

74. Følgende foranstaltninger er eksempler på supplerende foranstaltninger, som I kan overveje, når I når trin 4 "Vedtag supplerende foranstaltninger". Denne liste er ikke-udtømmende. I kan undersøge andre supplerende foranstaltninger. Fremtidige teknologiske, retlige eller organisatoriske udviklinger kan være med til at skabe nye supplerende foranstaltninger, som I kan overveje. Udvælgelse og gennemførelse af én eller flere af disse foranstaltninger vil ikke nødvendigvis og systematisk sikre, at jeres overførsel overholder standarden for væsentlig overensstemmelse, som krævet i EU-retten. I bør udvælge de supplerende foranstaltninger, der effektivt kan sikre dette beskyttelsesniveau for jeres overførsler.
75. Enhver supplerende foranstaltning kan kun anses for effektiv i medfør af EU-Domstolens dom "Schrems II", hvis og i det omfang den – i sig selv eller sammen med andre – afhjælper de specifikke mangler udpeget i jeres vurdering af situationen i tredjelandet med hensyn til dets lovgivning og praksis, som er gældende for jeres overførsel. Hvis I i sidste ende ikke kan sikre et reelt tilsvarende beskyttelsesniveau, må I ikke overføre personoplysningerne.
76. Som dataansvarlige eller databehandlere kan det allerede være et krav for jer at gennemføre nogle af foranstaltningerne beskrevet i dette bilag for at overholde GDPR. Dette betyder, at det kan være nødvendigt at indføre lignende foranstaltninger for personoplysninger, der er behandlet i EØS, og som overføres til en dataimportør omfattet af en afgørelse om tilstrækkelighed eller til andre tredjelande.⁷⁷

2.1 Tekniske foranstaltninger

77. Dette afsnit beskriver på en ikke-udtømmende måde eksempler på tekniske foranstaltninger, som kan supplere garantierne, der findes i overførselsværktøjer, jf. artikel 46 i GDPR, for at sikre overholdelse af det beskyttelsesniveau, som kræves under EU-retten i forbindelse med overførsel af personoplysninger til et tredjeland. Der vil især være behov for disse foranstaltninger, når lovgivningen i det pågældende land pålægger forpligtelser over for dataimportøren, som er i strid med garantierne, der findes i overførselsværktøjer, jf. artikel 46 i GDPR, og som kan bringe den kontraktlige garanti for et i det væsentlige tilsvarende beskyttelsesniveau mod adgang til disse oplysninger for de offentlige myndigheder i tredjelandet i fare.⁷⁸
78. For at skabe yderligere klarhed beskriver dette afsnit først nogle eksempler på scenarier, hvor nogle tekniske foranstaltninger potentielt kan være effektive for at sikre et i det væsentlige tilsvarende beskyttelsesniveau. Afsnittet fortsætter så med scenarier, hvor de tekniske foranstaltninger til sikring af dette beskyttelsesniveau ikke er konstateret.

⁷⁷ Artikel 5, stk. 2, i GDPR, artikel 32 i GDPR.

⁷⁸ C-311/18 (Schrems II), præmis 135.

Eksempler på scenarier, der henviser til tilfælde, hvor der er konstateret effektive foranstaltninger

79. De nedenfor anførte foranstaltninger har til hensigt at sikre, at adgangen til de overførte oplysninger for tredjelandes offentlige myndigheder ikke bringer effektiviteten af de fornødne garantier, der findes i overførselsværktøjer, jf. artikel 46 i GDPR, i fare. Disse foranstaltninger vil være nødvendige for at sikre et beskyttelsesniveau, der i det væsentlige svarer til det niveau, der er sikret i EØS, selv om de offentlige myndigheders adgang overholder loven i importørens land, hvor en sådan adgang i praksis går videre, end hvad der er nødvendigt og proportionelt i et demokratisk samfund.⁷⁹ Målet med disse foranstaltninger er at udelukke potentielt krænkende adgang ved at forhindre, at myndighederne identificerer de registrerede, udleder oplysninger om dem, fremhæver dem i en anden sammenhæng eller sammenligner de overførte data med andre datasæt, som bl.a. kan indeholde onlineidentifikatorer tilvejebragt af de enheder, applikationer, værktøjer og protokoller, som de registrerede benytter i andre sammenhænge.
80. Offentlige myndigheder i tredjelande kan forsøge på at tilgå overførte data
- a) under overførslen ved at tilgå de kommunikationslinjer, som bruges til at overføre dataene til modtagerlandet. Denne adgang kan være passiv, hvor kommunikationens indhold, muligvis efter en udvælgelsesproces, bare kopieres. Adgangen kan dog også være aktiv i den forstand, at de offentlige myndigheder griber ind i kommunikationsprocessen ved ikke kun at læse indholdet men også manipulere eller fjerne dele af det.
 - b) når den tiltænkte modtager af dataene er i besiddelse af dem ved enten at tilgå selve behandlingsenhederne eller ved at kræve, at datamodtageren lokaliserer og udtrækker relevante data og overdrager dem til myndighederne.
81. Dette afsnit overvejer scenarier, hvor foranstaltninger benyttes, som er effektive i begge tilfælde. Forskellige supplerende foranstaltninger kan finde anvendelse og være tilstrækkelige under de givne omstændigheder for en konkret overførsel, hvis kun én form for adgang planlægges, jf. lovgivningen i modtagerlandet. Dataeksportøren skal derfor omhyggeligt undersøge forpligtelserne pålagt dataimportøren med dennes støtte.

Som et eksempel er amerikanske dataimportører, der er omfattet af § 1881a i 50 USC (FISA sec. 702), direkte forpligtede til at tildele adgang til eller overdrage importerede personoplysninger, som de er i besiddelse af, som er i deres varetægt, eller som de har kontrol over. Kryptografiske nøgler, som er nødvendige for at gøre dataene forståelige, kan være omfattet heraf.

82. Scenarierne beskriver som eksempel specifikke omstændigheder og trufne foranstaltninger. Enhver ændring af scenarierne kan medføre forskellige konklusioner. Scenarierne henviser til situationer, hvor det er blevet konkluderet, at der først og fremmest er behov for supplerende

⁷⁹ Jf. artikel 47 og 52 i EU's charter om grundlæggende rettigheder, artikel 23, stk. 1, i GDPR samt Databeskyttelsesrådets henstilling nr. 02/2020 om europæiske væsentlige garantier for overvågningsforanstaltninger af 10. november 2020.

foranstaltninger, dvs. når problematisk lovgivning i praksis anvendes på den pågældende overførsel.

83. Dataansvarlige kan være nødt til at benytte nogle eller alle foranstaltningerne beskrevet heri, uanset beskyttelsesniveauet fastlagt i lovgivningen, som er gældende for dataimportøren, da de skal overholde artikel 25 og 32 i GDPR under overførselens konkrete omstændigheder. Med andre ord kan det være et krav, at eksportører skal gennemføre foranstaltningerne beskrevet i dette dokument, selv om deres dataimportører er omfattet af en afgørelse om tilstrækkelighed, på samme måde, som det kan være et krav, at dataansvarlige og databehandlere gennemfører dem, når data behandles inden for EØS.

Brugstilfælde 1: Datalagring til sikkerhedskopiering og andre formål, som ikke kræver adgang til ikke-krypterede data

84. En dataeksportør bruger en udbyder af værtstjenester i et tredjeland til at lagre personoplysninger f.eks. til sikkerhedskopiering.

Hvis

1. de behandlede personoplysninger bruger stærk kryptering inden overførslen, og importørens identitet er verificeret
2. krypteringsalgoritmen og dennes parameterisering (dvs. nøglelængde og driftstilstand, om relevant) lever op til det aktuelle tekniske niveau og kan anses for at være robust mod den kryptoanalyse, som udføres af de offentlige myndigheder i modtagerlandet, hvor der tages forbehold for deres tilgængelige ressourcer og tekniske kapaciteter (dvs. computerkraft til brute force-angreb)⁸⁰
3. krypteringens styrke og nøglelængden tager hensyn til den specifikke tidsperiode, hvorunder de krypterede personoplysningers fortrolighed skal bevares⁸¹

⁸⁰ Til vurderingen af krypteringsalgoritmers styrke, om de lever op til det aktuelle tekniske niveau, og om de er robuste mod den kryptoanalyse, der udføres over tid, kan dataeksportører benytte tekniske vejledninger offentliggjort af officielle cybersikkerhedsmyndigheder i EU og medlemsstaterne. Se f.eks. ENISA-rapporten "What is "state of the art" in IT security? ", 2019, <https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security>, retningslinjer fra det tyske forbundskontor for informationssikkerhed i dettes tekniske retningslinjer i TR-02102-serien og "[Algorithms, Key Size and Protocols Report \(2018\)](#)", H2020-ICT-2014 – Project 645421, D5.4, [ECRYPT-CSA](#), 02/2018" på <https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf>.

⁸¹ Kryptografiske algoritmers beskyttelseskapacitet falder over tid som følge af opdagelsen af nye kryptoanalytiske teknikker, fremkomsten af nye databehandlingsparadigmer som kvantedatabehandling og den generelle forøgelse af tilgængelig computerkraft, medmindre de anvendte algoritmer bevisligt er informationsteoretisk sikre. Dette gælder navnlig offentlige nøglealgoritmer, der i skrivende stund er almindeligt anvendt. Dataeksportøren skal derfor tage i betragtning, at offentlige myndigheder kan få adgang til krypterede oplysninger under de omstændigheder, der er beskrevet i punkt 80, og lagre dem, indtil deres ressourcer er tilstrækkelige til en dekryptering. Den supplerende foranstaltning kan kun anses for at være effektiv, hvis en sådan dekryptering og efterfølgende viderebehandling på dette tidspunkt ikke længere ville udgøre en krænkelse af registreredes rettigheder, f.eks. fordi oplysningerne ikke længere kan anvendes til at identificere dem direkte eller indirekte.

4. krypteringsalgoritmen er implementeret korrekt og af korrekt vedligeholdt software uden kendte sårbarheder, hvis overholdelse af den valgte algoritmes specifikation er bekræftet, f.eks. ved certificering
5. nøglerne forvaltes pålideligt (de genereres, administreres, lagres, om relevant, knyttes til identiteten for en tiltænkt modtager og ophæves),⁸² og
6. nøglerne forbliver udelukkende under kontrollen af dataeksportøren eller en enhed, som eksportøren har tillid til, i EØS eller under en jurisdiktion, der tilbyder et beskyttelsesniveau, der i det væsentlige svarer til det niveau, der er sikret i EØS

så vurderer Databeskyttelsesrådet, at den udførte kryptering udgør en effektiv supplerende foranstaltning.

Brugstilfælde 2: Overførsel af pseudonymiserede data

85. Først pseudonymiserer en dataeksportør de data, denne er i besiddelse af, derefter overfører den dataene til et tredjeland med henblik på analyse, f.eks. til forskningsformål.

Hvis

1. en dataeksportør overfører personoplysninger, som er behandlet på en sådan måde, at personoplysningerne ikke længere kan henføres til en bestemt registreret eller bruges til at udpege den registrerede i en større gruppe uden brug af yderligere oplysninger⁸³
2. de yderligere oplysninger forbliver udelukkende i dataeksportørens besiddelse og opbevares særskilt i en medlemsstat eller i et tredjeland, i en enheds besiddelse, som eksportøren har tillid til, i EØS eller under en jurisdiktion, der tilbyder et beskyttelsesniveau, der i det væsentlige svarer til det niveau, der er sikret i EØS
3. offentliggørelse eller uautoriseret brug af de yderligere oplysninger forhindres ved passende tekniske og organisatoriske garantier, og det sikres, at dataeksportøren beholder den udelukkende kontrol over algoritmen eller arkivet, som muliggør genidentifikation ved brug af de yderligere oplysninger
4. den dataansvarlige på baggrund af en grundig analyse af de pågældende data, der tager hensyn til de eventuelle oplysninger, som de offentlige myndigheder i modtagerlandet kan forventes at besidde og anvende, har fastlagt, at de pseudonymiserede personoplysninger ikke

⁸² NIST Special Publication 800-57, Recommendation for Key Management <https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final>

⁸³ I overensstemmelse med artikel 4, nr. 5), i GDPR: "“pseudonymisering”: behandling af personoplysninger på en sådan måde, at personoplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger, forudsat at sådanne supplerende oplysninger opbevares separat og er underlagt tekniske og organisatoriske foranstaltninger for at sikre, at personoplysningerne ikke henføres til en identificeret eller identificerbar fysisk person"; supplerende oplysninger kan bestå af tabeller, der sammenstiller pseudonymer med de identificerende attributter, de erstatter, kryptografiske nøgler eller andre parametre for transformationen af attributter eller oplysninger, der gør det muligt at henføre pseudonymiserede oplysninger til identificerede eller identificerbare fysiske personer.

kan henføres til en identificeret eller identificerbar fysisk person, selv hvis de krydshenvises med sådanne oplysninger

så vurderer Databeskyttelsesrådet, at den udførte pseudonymisering udgør en effektiv supplerende foranstaltning.

86. Bemærk, at faktorer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet, dennes fysiske placering eller vedkommendes interaktion med en internetbaseret tjeneste på bestemte tidspunkter⁸⁴, i mange situationer kan muliggøre identifikation af denne person, selv om vedkommendes navn, adresse eller andre tydelige identifikatorer udelades.
87. Dette er især tilfældet, når dataene omhandler brugen af informationstjenester (adgangstidspunkt, sekvensen af brugte funktioner, egenskaber for den anvendte enhed osv.). Disse tjenester kan ligesom importøren af personoplysninger være forpligtede til at give adgang til de samme offentlige myndigheder i deres jurisdiktion, som så sandsynligvis vil besidde data om brugen af disse informationstjenester for den/de person(er), de har udvalgt.
88. Desuden skal dataansvarlige som følge af, at brugen af nogle informationstjenester er offentlig grundet deres natur, eller fordi de kan udnyttes af parter med væsentlige ressourcer, være ekstra forsigtige, da de offentlige myndigheder i deres jurisdiktion sandsynligvis besidder data om brugen af informationstjenester for en person, de har udvalgt.
89. Hvis attributter, der er indeholdt i personoplysningerne, i forbindelse med pseudonymiseringen transformeres ved hjælp af en kryptografisk algoritme, gælder vejledningen i fodnote 80 og 81. Fremover anbefales det at afstå fra udelukkende at anvende kryptografi og anvende transformationer baseret på tabelopslag.

Brugstilfælde 3: Kryptering af data for at beskytte dem mod adgang for de offentlige myndigheder i importørens tredjeland, når de passerer mellem eksportøren og importøren

90. En dataeksportør ønsker at overføre data til en destination, hvor lovgivningen og/eller praksis tillader offentlige myndigheder adgang til data, når de passerer mellem eksportørens land og destinationslandet.

Hvis

1. en dataeksportør overfører personoplysninger til en dataimportør i en jurisdiktion, hvor lovgivningen og/eller praksis tillader de offentlige myndigheder adgang til data, mens de transporteres via internettet til dette tredjeland uden de europæiske væsentlige garantier for denne adgang, transportkryptering benyttes, hvor det sikres, at de anvendte krypteringsprotokoller lever op til det aktuelle tekniske niveau og giver effektiv beskyttelse mod aktive og passive angreb ved brug af ressourcer, som man ved, at de offentlige myndigheder i dette tredjeland har adgang til

⁸⁴ Artikel 4, nr. 1), i GDPR: "'personoplysninger': enhver form for information om en identificeret eller identificerbar fysisk person ('den registrerede'); ved identificerbar fysisk person forstås en fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator som f.eks. et navn, et identifikationsnummer, lokaliseringsdata, en onlineidentifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet".

2. parterne involveret i kommunikationen bliver enige om en troværdig certificeringsmyndighed eller infrastruktur for offentlige nøgler
3. der bruges særlige beskyttende og nye foranstaltninger mod aktive og passive angreb mod sende- og modtagesystemerne, der sikrer transportkryptering, herunder test for softwaresårbarheder og mulige bagdøre
4. personoplysninger også krypteres ende-til-ende på applikationslaget ved brug af de nyeste krypteringsmetoder i tilfælde af, at transportkrypteringen ikke i sig selv giver tilstrækkelig sikkerhed grundet erfaringer med sårbarheder ved den brugte infrastruktur eller software
5. krypteringsalgoritmen og dennes parameterisering (f.eks. nøglelængde og driftstilstand, om relevant) lever op til det aktuelle tekniske niveau og kan anses for at være robust mod den kryptoanalyse, som udføres af de offentlige myndigheder, når data passerer igennem til dette tredjeland, under hensyntagen til deres tilgængelige ressourcer og tekniske kapaciteter (f.eks. computerkraft til brute force-angreb) (se fodnote 80 ovenfor)⁸⁵
6. krypteringens styrke tager hensyn til den specifikke tidsperiode, hvorunder de krypterede personoplysningers fortrolighed skal bevares
7. krypteringsalgoritmen er implementeret korrekt og af korrekt vedligeholdt software uden kendte sårbarheder, hvis overholdelse af den valgte algoritmes specifikation er bekræftet, f.eks. ved certificering
8. nøglerne forvaltes pålideligt (de genereres, administreres, lagres, om relevant, knyttes til identiteten af en tiltænkt modtager og ophæves) af eksportøren eller en enhed, som eksportøren har tillid til, under en jurisdiktion, der tilbyder et reelt tilsvarende beskyttelsesniveau

så vurderer Databeskyttelsesrådet, at transportkryptering, hvis der er behov for det i kombination med ende-til-ende-kryptering af indhold, udgør en effektiv supplerende foranstaltning.

Brugstilfælde 4: Beskyttet modtager

91. En dataeksportør overfører personoplysninger til en dataimportør i et tredjeland, som er særligt beskyttet under det lands lovgivning, f.eks. med henblik på at samarbejde om at give en patient lægebehandling eller for at levere juridiske tjenesteydelser til en klient.

Hvis

1. loven i tredjelandet fritager en dataimportør, der er bosat deri, fra potentielt at overskride adgang til data, som modtageren besidder til det pågældende formål, f.eks. på baggrund af en tavshedspligt, som dataimportøren er underlagt
2. den fritagelse omfatter alle oplysninger, som dataimportøren er i besiddelse af, og som kan benyttes til at omgå beskyttelsen af fortrolige oplysninger (kryptografiske nøgler, kodeord, andre legitimationsoplysninger osv.)
3. dataimportøren ikke beskæftiger en databehandler på en måde, der gør det muligt for offentlige myndigheder at tilgå dataene, mens databehandleren er i besiddelse af dem, eller hvis dataimportøren videresender dataene til en anden enhed, som ikke er beskyttet, på baggrund af overførselsværktøjer, jf. artikel 46 i GDPR

⁸⁵ Se fodnote 80 med henvisninger til tekniske vejledninger offentliggjort af officielle cybersikkerhedsmyndigheder i EU og medlemsstaterne.

4. personoplysningerne er krypterede, inden de overføres med en metode, der lever op til det aktuelle tekniske niveau, som sikrer, at kryptering ikke er muligt uden kendskab til krypteringsnøglen (ende-til-ende-kryptering), under hele tidsperioden, hvor dataene skal beskyttes
5. krypteringsnøglen udelukkende er i den beskyttede dataimportørs besiddelse, og muligvis eksportøren selv eller en anden enhed, som eksportøren har tillid til og befinder sig i EØS, eller en jurisdiktion, der tilbyder et beskyttelsesniveau, der i det væsentlige svarer til det niveau, der er sikret i EØS, og er passende sikret mod uautoriseret brug eller offentliggørelse via tekniske og organisatoriske foranstaltninger, som lever op til det aktuelle tekniske niveau, og
6. dataeksportøren pålideligt har fastlagt, at krypteringsnøglen, vedkommende planlægger at bruge, svarer til krypteringsnøglen, som modtageren har

så vurderer Databeskyttelsesrådet, at den udførte transportkryptering udgør en effektiv supplerende foranstaltning.

Brugstilfælde 5: Delt behandling eller behandling ved flere parter

92. Dataeksportøren ønsker, at personoplysninger behandles i et samarbejde mellem to eller flere uafhængige behandlere, som befinder sig i forskellige jurisdiktioner, uden at dataenes indhold afsløres for dem. Inden overførslen deles dataene på en måde, så ingen del, som en enkelt behandler modtager, er tilstrækkelig til at genopbygge personoplysninger helt eller delvist. Dataeksportøren modtager resultatet af behandlingen fra hver behandler individuelt og sammensætter de modtagne stykker for at nå det endelige resultat, der kan udgøre personoplysninger eller aggregerede data.

Hvis

1. en dataeksportør behandler personoplysninger på en sådan måde, at de deles i to eller flere dele, som hver ikke længere kan fortolkes eller henføres til en specifik registreret person uden brug af yderligere oplysninger
2. hver af stykkerne overføres til en separat behandler, som befinder sig i en anden jurisdiktion
3. behandlerne vælger at behandle dataene i fællesskab, dvs. ved brug af sikker flerpartsberegning på en måde, så ingen oplysninger, som de ikke besad inden beregningen, afsløres for nogen af dem
4. algoritmen anvendt til den delte beregning er sikker mod aktive angreb
5. den dataansvarlige på baggrund af en grundig analyse af de pågældende data, der tager hensyn til de manglende oplysninger, som de offentlige myndigheder i modtagerlandene kan forventes at besidde og anvende, har fastlagt, at de dele af de personoplysninger, denne overfører til databehandlerne, ikke kan henføres til en identificeret eller identificerbar fysisk person, selv hvis de krydshenvises med sådanne oplysninger
6. der ikke er bevis for samarbejde mellem de offentlige myndigheder, der hører til i de forskellige jurisdiktioner, hvor hver behandler befinder sig, hvilket ville give dem mulighed for at tilgå alle sæt med personoplysninger, som behandlerne besidder, og gør dem i stand til at rekonstruere og udnytte personoplysningernes indhold på en tydelig måde i situationer, hvor en sådan udnyttelse ikke ville overholde det væsentlige i registreredes grundlæggende rettigheder og frihedsrettigheder. På tilsvarende vis bør offentlige myndigheder i begge lande ikke have beføjelser til at tilgå personoplysninger, som databehandlere i alle berørte jurisdiktioner besidder.

så vurderer Databeskyttelsesrådet, at den udførte delte behandling udgør en effektiv supplerende foranstaltning.

Eksempler på scenarier, der henviser til tilfælde, hvor der ikke er konstateret effektive foranstaltninger

93. Foranstaltningerne beskrevet nedenfor under visse scenarier ville ikke være effektive til at sikre et reelt tilsvarende beskyttelsesniveau for dataene, der overføres til tredjelandet. De ville derfor ikke være kvalificeret som passende supplerende foranstaltninger.

Brugstilfælde 6: Overførsel til cloud-udbydere eller andre databehandlere, som kræver adgang til ikke-krypterede data

94. En dataeksportør overfører personoplysninger, enten ved elektronisk overførsel eller ved at gøre dem tilgængelige for en cloud-udbyder eller anden databehandler til at behandle personoplysninger i et tredjeland i henhold til dennes anvisninger (f.eks. med henblik på teknisk support eller enhver form for cloud-behandling), og disse data er ikke pseudonymiseret – eller kan ikke pseudonymiseres – som beskrevet i brugstilfælde 2 eller krypteret som beskrevet i brugstilfælde 1, fordi behandlingen kræver adgang til ikke-krypterede data.

Hvis

1. en dataansvarlig overfører personoplysninger til en cloud-udbyder eller anden databehandler
2. cloud-udbyderen eller den anden databehandler skal bruge adgang til ikke-krypterede data for at udføre den tildelte opgave
3. beføjelsen tildelt de offentlige myndigheder i modtagerlandet til at tilgå de pågældende overførte data går videre, end hvad der er nødvendigt og proportionelt i et demokratisk samfund, når problematisk lovgivning i praksis gælder for de pågældende overførsler (se trin 3).⁸⁶

så er Databeskyttelsesrådet, på baggrund af det aktuelle tekniske niveau, ikke i stand til at forestille sig en effektiv teknisk foranstaltning, som kan forhindre denne adgang i at krænke den registreredes grundlæggende rettigheder. Databeskyttelsesrådet udelukker ikke, at senere tekniske udviklinger kan tilbyde foranstaltninger, som opnår de tiltænkte forretningsmæssige formål, uden at kræve adgang til ikke-krypterede data.

95. I de pågældende scenarier, hvor ikke-krypterede personoplysninger teknisk set er nødvendige for at levere databehandlerens tjenesteydelser, udgør transportkryptering og kryptering af data i hvile, selv ved brug af begge krypteringsformer, ikke en supplerende foranstaltning, som sikrer et reelt tilsvarende beskyttelsesniveau, hvis dataimportøren er i besiddelse af de kryptografiske nøgler.

⁸⁶ Jf. artikel 47 og 52 i EU's charter om grundlæggende rettigheder, artikel 23, stk. 1, i GDPR samt Databeskyttelsesrådets henstilling nr. 02/2020 om europæiske væsentlige garantier for overvågningsforanstaltninger af 10. november 2020.

Brugstilfælde 7: Overførsel af personoplysninger til forretningsmæssige formål, herunder i form af fjernadgang

96. En dataeksportør overfører personoplysninger til enheder – i et tredjeland, så de kan bruges til fælles forretningsmæssige formål – enten ved elektronisk overførsel eller ved at gøre dem tilgængelige for dataimportørens fjernadgang – og disse data er ikke pseudonymiseret – eller kan ikke pseudonymiseres – som beskrevet i brugstilfælde 2 eller krypteret som beskrevet i brugstilfælde 1, fordi behandlingen kræver adgang til ikke-krypterede data. Én typisk sammensætning kan bestå af en dataansvarlig eller databehandler, som er etableret inden for en medlemsstat, der overfører personoplysninger til en dataansvarlig eller databehandler i et tredjeland, der hører til den samme koncern, eller en gruppe af foretagender, som udøver en fælles økonomisk aktivitet. Dataimportøren kan for eksempel bruge de data, denne modtager, til at levere personaletjenester for dataeksportøren, til hvilke der skal bruges data om menneskelige ressourcer, eller til at kommunikere med dataeksportørens kunder, som bor i Den Europæiske Union, via telefon eller e-mail.

Hvis

1. en dataeksportør overfører personoplysninger til en dataimportør i et tredjeland ved at gøre dem tilgængelige i et informationssystem på en måde, der giver importøren direkte adgang til data efter eget valg, eller ved at overføre dem direkte, enkeltvist eller som massedata ved brug af en kommunikationstjeneste
2. importøren⁸⁷ behandler de ikke-krypterede data i tredjelandet (herunder til sine egne formål, når importøren er en dataansvarlig)
3. beføjelsen tildelt de offentlige myndigheder i modtagerlandet til at tilgå de overførte data går videre, end hvad der er nødvendigt og proportionelt i et demokratisk samfund, når problematisk lovgivning i praksis gælder for de pågældende overførsler (se trin 3).

så er Databeskyttelsesrådet ikke i stand til at forestille sig en effektiv teknisk foranstaltning, som kan forhindre denne adgang i at krænke den registreredes grundlæggende rettigheder.

97. I de pågældende scenarier, hvor ikke-krypterede personoplysninger teknisk set er nødvendige for at levere databehandlerens tjenesteydelser, udgør transportkryptering og kryptering af data i hvile, selv ved brug af begge krypteringsformer, ikke en supplerende foranstaltning, som sikrer et reelt tilsvarende beskyttelsesniveau, hvis dataimportøren er i besiddelse af de kryptografiske nøgler.

⁸⁷ Hvad enten der er tale om en dataansvarlig eller databehandler i et tredjeland, som modtager eller får adgang til personoplysninger, der er overført fra EØS.

2.2 Yderligere kontraktmæssige foranstaltninger

98. Disse foranstaltninger vil generelt bestå af unilaterale, bilaterale eller multilaterale⁸⁸ kontraktmæssige forpligtelser.⁸⁹ Hvis et overførselsværktøj, jf. artikel 46 i GDPR, benyttes, vil det i de fleste tilfælde allerede indeholde flere af dataeksportørens og dataimportørens (for det meste kontraktmæssige) forpligtelser, der er tiltænkt som garantier for personoplysningerne.⁹⁰

99. I nogle situationer kan disse foranstaltninger supplere og forstærke de garantier, som overførselsværktøjet og den relevante lovgivning i tredjelandet kan levere, når disse under hensyntagen til omstændighederne for overførslen ikke opfylder alle de betingelser, som er krævet for at sikre et beskyttelsesniveau, der i det væsentlige svarer til det, der er sikret inden for EØS. Såfremt de kontraktmæssige foranstaltninger har en natur, som generelt ikke er i stand til at binde myndighederne i det pågældende tredjeland, når de ikke er parter i kontrakten,⁹¹ kan det ofte være nødvendigt at kombinere disse foranstaltninger med andre tekniske og organisatoriske foranstaltninger, der kan levere det krævede beskyttelsesniveau. Udvælgelse og gennemførelse af én eller flere af disse foranstaltninger vil ikke nødvendigvis og systematisk sikre, at jeres overførsel overholder standarden for væsentlig overensstemmelse, som krævet i EU-retten.

100. Alt efter hvilke kontraktmæssige foranstaltninger, som allerede er inkluderet i overførselsværktøjet, jf. artikel 46 i GDPR, der benyttes, kan yderligere kontraktmæssige foranstaltninger også være en hjælp til at gøre EØS-baserede dataeksportører opmærksomme på nye udviklinger, som påvirker produktionen af dataene, der overføres til tredjelande.

101. Som tidligere nævnt vil kontraktmæssige foranstaltninger ikke kunne udelukke anvendelsen af lovgivningen i et tredjeland, som ikke opfylder Databeskyttelsesrådets standard om europæiske væsentlige garantier i de tilfælde, hvor lovgivningen forpligter importører til at overholde påbuddene, de modtager fra offentlige myndigheder om at videregive data.⁹²

102. Nogle eksempler på disse potentielle kontraktmæssige foranstaltninger er angivet nedenfor og klassificeres ud fra deres natur.

Fastlæggelse af den kontraktmæssige forpligtelse om at benytte særlige tekniske foranstaltninger

103. Alt efter overførselens særlige omstændigheder (herunder den praktiske anvendelse af tredjelandets lovgivning) kan det være nødvendigt, at kontrakten fastlægger, at specifikke

⁸⁸ F.eks. i bindende virksomhedsregler, som, uanset hvad, bør regulere nogle af de nedenstående foranstaltninger.

⁸⁹ De vil have en privat natur og vil ikke betragtes som internationale aftaler under international offentlig ret. Som følge heraf vil de normalt ikke binde tredjelandets offentlige myndighed som ikke-kontraherende parter til kontrakten, når den indgås med private organer i tredjelande, hvilket Domstolen understregede i sin dom C-311/18 (Schrems II), præmis 125.

⁹⁰ Se dom C-311/18 (Schrems II), præmis 137, hvor Domstolen som en konsekvens anerkendte, at standardkontraktbestemmelser indeholder "effektive mekanismer, som i praksis gør det muligt at sikre, at det i EU-retten krævede beskyttelsesniveau overholdes, og at overførslerne af personoplysninger på grundlag af sådanne bestemmelser suspenderes eller forbydes, hvis disse bestemmelser overtrædes, eller hvis det er umuligt at overholde dem"; se også præmis 148.

⁹¹ C-311/18 (Schrems II), præmis 125.

⁹² EU-Domstolens dom C-311/18 (Schrems II), præmis 132.

tekniske foranstaltninger skal gennemføres, før overførsler kan finde sted (se de tekniske foranstaltninger, der foreslås ovenfor).

104. Betingelser for effektivitet:

- Denne standardbestemmelse kan være effektiv i de situationer, hvor behovet for tekniske foranstaltninger er identificeret af eksportøren. De skal derefter fastlægges i en juridisk form for at sikre, at importøren også forpligter sig til at etablere de nødvendige tekniske foranstaltninger, hvis det er nødvendigt.

Forpligtelser om gennemsigtighed:

105. Eksportøren kan føje bilag til kontrakten med oplysninger, som importøren efter bedste formåen har angivet inden kontraktens indgåelse, om dataadgang for offentlige myndigheder, herunder inden for efterretning, hvis lovgivningen overholder Databeskyttelsesrådets europæiske væsentlige garantier, i destinationslandet. Dette kan hjælpe dataeksportøren med at opfylde sin forpligtelse om at dokumentere sin vurdering af beskyttelsesniveauet i tredjelandet. Det kan også understrege importørens forpligtelse til at bistå eksportøren med dennes vurdering og dennes ansvar for at give oplysninger, der er objektive, pålidelige, relevante, verificerbare og offentligt tilgængelige eller på anden måde tilgængelige oplysninger.

106. Det kan for eksempel være et krav, at importøren:

- (1) opregner de love og forskrifter i destinationslandet, som er gældende for importøren eller dennes (under)databehandlere, som ville tillade, at offentlige myndigheder får adgang til de personoplysninger, der overføres, navnlig i forbindelse med efterretning, retshåndhævelse, administrativt og lovbestemt tilsyn, som finder anvendelse for de overførte data
- (2) hvis der ikke findes lovgivning om offentlige myndigheders dataadgang, angiver oplysninger og statistikker baseret på importørens erfaringer eller rapporter fra forskellige kilder (f.eks. partnere, åbne kilder, national retspraksis og afgørelser fra tilsynsorganer) om offentlige myndigheders adgang til personoplysninger i situationer lig den pågældende dataoverførsel (dvs. inden for det specifikke regulerede område; vedrørende den enhedstype, som dataimportøren er klassificeret som, osv.)
- (3) angiver, hvilke foranstaltninger der er truffet for at forhindre adgangen til de overførte data (om nogen)
- (4) leverer tilstrækkeligt detaljerede oplysninger om alle anmodninger om adgang til personoplysninger fra offentlige myndigheder, som importøren har modtaget over en specifik tidsperiode,⁹³ navnlig områderne angivet i ovenstående nr. 1), og som består af oplysninger om de modtagne anmodninger, de anmodede data, organet, der har sendt anmodningen, og det retslige grundlag for videregivelsen, og i hvilket omfang importøren har videregivet dataanmodningen⁹⁴

⁹³ Tidsperioden bør afhænge af risikoen for rettighederne og frihedsrettighederne for de registrerede, hvis data overføres — f.eks. det sidste år inden lukning af dataeksportinstrumentet ved dataeksportøren

⁹⁴ Overholdelse af denne anmodning udgør som sådan ikke et passende beskyttelsesniveau. På samme tid understreger enhver uhensigtsmæssig offentliggørelse, som faktisk har fundet sted, nødvendigheden af at gennemføre supplerende foranstaltninger.

(5) angiver, om og i hvilket omfang importøren har et lovbestemt forbud mod at videregive oplysningerne anført i ovenstående nr. 1)-5).

107. Disse oplysninger kan videregives via strukturerede spørgeskemaer, som importøren udfylder og underskriver, og hertil kommer importørens kontraktmæssige forpligtelse om inden for en fastlagt tidsperiode at erklære eventuelle ændringer af disse oplysninger, hvilket er gældende praksis for processer vedrørende rettidig omhu.

108. Betingelser for effektivitet:

- Importøren skal efter bedste overbevisning, og efter denne har gjort sit bedste for at indhente dem, være i stand til at videregive disse typer af oplysninger til eksportøren.
- Denne forpligtelse pålagt importøren er en måde at sikre, at eksportøren bliver og forbliver opmærksom på de risici, som er forbundet med overførslen af data til et tredjeland. Det vil dermed give eksportøren mulighed for at afstå fra at indgå kontrakten, eller hvis oplysningerne ændrer sig efter dennes indgåelse, opfylde dennes forpligtelse om at suspendere overførslen og/eller opsige kontrakten, hvis loven i tredjelandet, garantierne indeholdt i det anvendte overførselsværktøj, jf. artikel 46 i GDPR, og alle yderligere garantier, som denne har truffet, ikke længere kan sikre et beskyttelsesniveau, der i det væsentlige svarer til det, der er sikret inden for EØS. Denne forpligtelse kan hverken begrunde importørens offentliggørelse af personoplysninger eller føre til forventninger om, at der ikke vil være flere adgangsanmodninger.

109. Eksportøren kan også tilføje standardbestemmelser, hvormed importøren certificerer, at 1) denne ikke bevidst har oprettet bagdøre eller lignende programmering, som kan bruges til at få adgang til systemet og/eller personoplysninger 2) denne ikke bevidst har oprettet eller ændret sine forretningsprocesser på en måde, som giver adgang til personoplysninger eller systemer, og 3) national lovgivning eller regeringspolitikker ikke kræver, at importøren opretter eller vedligeholder bagdøre eller giver adgang til personoplysninger eller systemer, eller at importøren skal være i besiddelse af eller overdrage krypteringsnøglen.⁹⁵

110. Betingelser for effektivitet:

- Tilstedeværelsen af lovgivning eller regeringspolitikker, der forhindrer importører fra at offentliggøre disse oplysninger, kan gøre denne standardbestemmelse ineffektiv. Importøren vil dermed ikke være i stand til at indgå kontrakten eller kan have brug for at underrette eksportøren om sin manglende evne til fortsat at overholde sine kontraktmæssige forpligtelser.
- Kontrakten skal indeholde sanktioner og/eller en mulighed for, at eksportøren kan opsige kontrakten med kort varsel i de tilfælde, hvor importøren ikke afslører eksistensen af en bagdør eller lignende programmering eller manipulerede forretningsprocesser eller et krav om at implementere disse eller ikke omgående informerer eksportøren, når denne bliver bekendt med deres eksistens.

⁹⁵ Denne standardbestemmelse er vigtig for at sikre et passende niveau for beskyttelse af de overførte personoplysninger og bør normalt være et krav.

- Under omstændigheder, hvor dataimportøren videregav personoplysninger overført i strid med tilsagnene omfattet af det valgte overførselsværktøj, kan kontrakten også omfatte erstatning fra dataimportøren til en registreret for eventuel materiel og immateriel skade, der er lidt.

111. Eksportøren kan forstærke sin beføjelse til at udføre kontroller⁹⁶ eller inspektioner af importørens databehandlingsfaciliteter på stedet og/eller fjernt for at bekræfte, om data blev videregivet til offentlige myndigheder og under hvilke forhold (adgang, som ikke går videre, end hvad der er nødvendigt og proportionelt i et demokratisk samfund), f.eks. ved at fastlægge et kort varsel og mekanismer, som sikrer hurtige indsatser for inspektionsorganer og styrker eksportørens selvstændighed ved valg af inspektionsorganer.

112. Betingelser for effektivitet:

- Kontrollens omfang bør juridisk og teknisk omfatte enhver behandling, som importørens databehandlere eller underdatabehandlere udfører på personoplysningerne overført i tredjelandet, for at den har en fuld virkning.
- Adgangslogfiler og anden lignende dokumentation bør være sikret mod manipulation (f.eks. bør det sikres, at de ikke kan ændres, ved brug af de nyeste krypteringsteknikker, f.eks. hashing, og også systematisk overføres til eksportøren med jævne mellemrum), så kontrolløren kan finde bevis for offentliggørelsen. Adgangslogfiler og anden lignende dokumentation bør også sondre mellem adgang som følge af almindelige forretningsaktiviteter og adgang grundet påbud eller adgangsanmodninger.

113. Da lovgivningen og praksissen i importørens tredjeland oprindeligt blev vurderet til at levere et beskyttelsesniveau, der reelt svarer til det, der er sikret inden for EU, for data, som overføres af eksportøren, kunne eksportøren stadig styrke dataimportørens forpligtelse til, i tilfælde af en ændring af situationen, omgående at informere dataeksportøren om dennes manglende evne til at overholde de kontraktmæssige forpligtelser og som følge heraf den krævede standard om et "reelt tilsvarende beskyttelsesniveau".⁹⁷

114. Denne manglende overholdelse kan være et resultat af ændringer af tredjelandets lovgivning eller praksis.⁹⁸ Standardbestemmelserne kan fastlægge specifikke og strenge tidsgrænser og procedurer for den hurtige suspendering af overførslen af data og/eller opsigelsen af kontrakten

⁹⁶ Se f.eks. standardbestemmelse 5, litra f), i afgørelse 2010/87/EU om standardkontraktbestemmelserne mellem dataansvarlige og databehandlere. Kontrollerne kan også gennemføres under et adfærdskodeks eller igennem certificering.

⁹⁷ Standardbestemmelse 5, litra a) og litra d), nr. i), i afgørelse 2010/87/EU om standardkontraktbestemmelser.

⁹⁸ Se C-311/18 (Schrems II), præmis 139, hvor Domstolen udtaler, at selv om "standardbestemmelse 5, litra d), nr. i), i øvrigt giver modtageren af overførslen af personoplysninger mulighed for ikke at give den dataansvarlige, som er etableret i Unionen, meddelelse om en retshåndhævende myndigheds retligt bindende anmodning om videregivelse af personoplysninger, såfremt der findes lovgivning, som forbyder ham dette, som f.eks. et forbud ifølge strafferetten med henblik på at sikre fortrolighed i efterforskningssager, har han ikke desto mindre i henhold til standardbestemmelse 5, litra a), pligt til at underrette den dataansvarlige om, at han ikke er i stand til at overholde standardbestemmelserne om databeskyttelse."

og importørens returnering eller sletning af de modtagne data. Registrering af modtagne anmodninger, deres omfang og effektiviteten af de foranstaltninger, der er vedtaget for at imødegå dem, bør give eksportøren tilstrækkelige indikatorer til at udøve sin pligt om at suspendere eller afslutte overførslen og/eller opsige kontrakten.

115. Betingelser for effektivitet:

- Meddelelsen skal finde sted, inden der tildes adgang til dataene. Ellers kan enkeltpersonens rettigheder allerede være krænket, når eksportøren modtager meddelelsen, hvis anmodningen er baseret på love i tredjelandet, der overskrider det databeskyttelsesniveau, som EU-retten garanterer. Meddelelsen kan stadig forhindre fremtidige overtrædelser og gøre det muligt for eksportøren at udøve sin pligt om at suspendere overførslen af personoplysninger til tredjelandet og/eller ophæve kontrakten.
- Dataimportøren skal overvåge alle retslige eller politiske udviklinger, der kan føre til, at denne ikke kan overholde sine forpligtelser, og omgående meddele dataeksportøren om sådanne ændringer og udviklinger inden deres gennemførelse, hvis muligt, så dataeksportøren kan indhente dataene fra dataimportøren.
- Standardbestemmelserne bør indeholde en hurtig mekanisme, hvorved dataeksportøren giver dataimportøren tilladelse til omgående at sikre eller returnere dataene til dataeksportøren eller, hvis dette ikke er muligt, slette eller på sikker vis kryptere dataene uden nødvendigvis at vente på eksportørens anvisninger, hvis en specifik grænse⁹⁹, som dataeksportøren og dataimportøren har aftalt, overholdes. Importøren bør gennemføre denne mekanisme fra begyndelsen af dataoverførslen og teste den regelmæssigt for at sikre, at den kan anvendes med kort varsel.
- Andre standardbestemmelser kan give eksportøren mulighed for at overvåge importørens overholdelse af disse forpligtelser via kontroller, inspektioner og andre bekræftende foranstaltninger og håndhæve dem via sanktioner pålagt importøren og/eller eksportørens kapacitet til at suspendere overførslen og/eller opsige kontrakten omgående.

116. Hvis tredjelandets nationale lovgivning tillader det, kan kontrakten forstærke importørens forpligtelser om gennemsigtighed ved at fastlægge en "Warrant Canary"-metode (kanariefuglsgaranti), hvor importøren forpligter sig til regelmæssigt at offentliggøre (dvs. mindst hver 24. time) en kryptografisk signeret meddelelse, der oplyser eksportøren om, at denne fra en bestemt dato og tidspunkt ikke har modtaget noget påbud om at videregive personoplysninger eller lignende. En manglende ajourføring af denne meddelelse vil antyde over for eksportøren, at importøren kan have modtaget et påbud.

117. Betingelser for effektivitet:

- Tredjelandets lovgivning skal tillade, at dataimportøren kan udsende denne form for passiv meddelelse til eksportøren.
- Dataeksportøren skal automatisk overvåge "Warrant Canary"-meddelelserne.

⁹⁹ Denne grænse bør sikre, at registrerede fortsat sikres et beskyttelsesniveau, der i det væsentlige svarer til det niveau, der er sikret i EØS.

- Dataimportøren skal sikre, at dennes private nøgle, der signerer en "Warrant Canary", opbevares sikkert, og at den ikke kan tvinges til at udsende en falsk "Warrant Canary" jf. tredjelandets lovgivning. Til dette formål kan det være brugbart, hvis der er brug for flere signaturer fra forskellige personer, og/eller "Warrant Canary" udstedes af en person, som ikke er omfattet af tredjelandets jurisdiktion.

Forpligtelser om at træffe specifikke foranstaltninger

118. Importøren kan forpligte sig til at gennemgå lovligheden af et påbud om at videregive data jf. lovgivningen i destinationslandet, navnlig om det indgår i beføjelserne tildelt den anmodende offentlige myndighed, og anfægte påbuddet, hvis denne efter en omhyggelig vurdering konkluderer, at der er et juridisk grundlag i destinationslandets lovgivning til at gøre dette. Når et påbud anfægtes, bør dataimportøren tilstræbe midlertidige foranstaltninger, der kan suspendere påbuddets virkninger, indtil domstolen har truffet afgørelse om sagens realiteter. Importøren ville være forpligtet til ikke at meddele de anmodede personoplysninger, indtil det er et krav under gældende procedureregler, at de gør det. Dataimportøren ville også forpligte sig til levere den minimalt tilladte mængde af oplysninger på baggrund af en rimelig fortolkning af påbuddet, når vedkommende svarer på påbuddet.

119. Betingelser for effektivitet:

- Tredjelandets retsorden skal tilbyde andre effektive juridiske muligheder for at anfægte påbud om at videregive data.
- Denne standardbestemmelse vil også tilbyde en meget begrænset ekstra beskyttelse, da et påbud om at videregive data kan være lovligt under tredjelandets retsorden, men denne retsorden opfylder muligvis ikke EU's standarder. Denne kontraktmæssige foranstaltning vil derfor være nødt til at supplere andre supplerende foranstaltninger.
- Anfægtelserne af påbuddene skal have en opsættende virkning under tredjelandets lovgivning. Ellers ville offentlige myndigheder stadig have adgang til enkeltpersonernes data, og alle efterfølgende handlinger, som er til enkeltpersonens fordel, ville have den begrænsede virkning at give vedkommende mulighed for at kræve erstatning for de negative virkninger som følge af videregivelsen af dataene.
- Importøren ville være nødt til at gøre sine bedste bestræbelser på at dokumentere og påvise de handlinger, denne har foretaget, over for eksportøren for at opfylde denne forpligtelse.

120. I samme situation som beskrevet ovenfor kan importøren forpligte sig til at oplyse den anmodende offentlige myndighed om påbuddets uforenelighed med garantierne indeholdt i overførselsværktøjet, jf. artikel 46 i GDPR¹⁰⁰, og importørens resulterende modstridende

¹⁰⁰ For eksempel fastlægger standardkontraktbestemmelserne, at databehandlingen, herunder overførslen af data, har været og fortsat udføres i overensstemmelse med "den gældende databeskyttelseslovgivning". Loven defineres som "den lovgivning, der beskytter fysiske personers grundlæggende rettigheder og frihedsrettigheder, især deres ret til beskyttelse af privatlivets fred, med hensyn til behandling af personoplysninger, og som gælder for en registeransvarlig i den medlemsstat, hvor dataeksportøren er etableret". EU-Domstolen bekræfter, at GDPR's bestemmelser læst sammen med EU's charter om grundlæggende rettigheder udgør en del af denne lovgivning, jf. EU-Domstolen C-311/18 (Schrems II), præmis 138.

forpligtelser. Importøren ville på samme tid og så hurtigt som muligt meddele eksportøren og/eller den kompetente tilsynsmyndighed fra EØS, så vidt det er muligt under tredjelandets retsorden.

121. Betingelser for effektivitet:

- Sådanne oplysninger om beskyttelsen, der tillægges ved EU-retten, og modstridende forpligtelser bør have nogen juridisk virkning i tredjelandets retsorden, såsom en retlig eller administrativ gennemgang af påbuddet eller adgangsmodningen, krav om en retskendelse og/eller midlertidig suspendering af påbuddet, for at beskytte dataene i større grad.
- Landets retssystem må ikke forhindre importøren i at meddele eksportøren eller som minimum den kompetente tilsynsmyndighed fra EØS omkring det modtagne påbud eller adgangsmodningen.
- Importøren ville være nødt til at gøre sine bedste bestræbelser på at dokumentere og påvise de handlinger, denne har foretaget, over for eksportøren for at opfylde denne forpligtelse.

Bemyndigelse af registrerede til at udøve deres rettigheder

122. Kontrakten kan angive, at personoplysninger, som overføres i ren tekst som led i det normale forretningsforløb (herunder i støtteforløb), kun må tilgås med eksportørens og/eller den registreredes udtrykkelige eller implicitte samtykke i forbindelse med en specifik adgang til oplysninger.

123. Betingelser for effektivitet:

- Denne standardbestemmelse kan være effektiv i de situationer, hvor importører modtager anmodninger fra offentlige myndigheder om at samarbejde på et frivilligt grundlag, i modsætning til f.eks. offentlige myndigheders dataadgang, som finder sted uden dataimportørens viden eller mod dennes vilje.
- I nogle situationer kan den registrerede ikke have mulighed for at modsige adgangen eller afgive et samtykke, som opfylder alle betingelserne fastlagt i EU-retten (frivillig, specifik, informeret og utvetydig) (f.eks. i tilfælde af medarbejdere)¹⁰¹.
- Nationale forskrifter eller politikker, som pålægger importøren ikke at meddele påbuddet om adgang, kan gøre denne standardbestemmelse ineffektiv, medmindre den kan understøttes af tekniske metoder, som kræver eksportørens eller den registreredes indsats, for at dataene i ren tekst bliver tilgængelige. Sådanne tekniske foranstaltninger om begrænsning af adgang kan påtænkes, navnlig hvis adgangen kun tildeles i specifikke støtte- eller servicetilfælde, men selve dataene lagres inden for EØS.

124. Kontrakten kan forpligte importøren og/eller eksportøren til omgående at underrette den registrerede om den modtagne anmodning eller påbud fra tredjelandets offentlige myndigheder eller om importørens manglende evne til at overholde de kontraktmæssige forpligtelser, som giver den registrerede mulighed for at indhente oplysninger og en effektiv klageadgang (f.eks. ved

¹⁰¹ Artikel 4, nr. 11), i GDPR.

at indgive en klage til dennes kompetente tilsynsmyndighed og/eller retlige myndighed og påvise vedkommendes søgsmålskompetencer ved domstolene i tredjelandet), herunder erstatning fra dataimportøren for eventuel materiel og immateriel skade, der er lidt på grund af videregivelsen af vedkommendes personoplysninger overført under det valgte overførselsværktøj i strid med tilsagnene heri.

125. Betingelser for effektivitet:

- Denne notifikation kan advare den registrerede, når tredjelandes offentlige myndigheder potentielt har adgang til vedkommendes data. Det kan dermed give den registrerede mulighed for at indhente yderligere oplysninger fra eksportørerne og indgive en klage til dennes kompetente tilsynsmyndighed. Denne standardbestemmelse kan også afhjælpe og kompensere nogle af de vanskeligheder, som en enkeltperson kan blive udsat for ved påvisning af dennes søgsmålskompetencer (*locus standi*) ved domstolene i tredjelandet for at anfægte offentlige myndigheders adgang til vedkommendes data.
- National lovgivning og nationale politikker kan forhindre denne notifikation af den registrerede. Eksportøren og importøren kan ikke desto mindre forpligte sig til at informere den registrerede, idet at restriktionerne for videregivelsen af data ophæves, og at gøre deres bedste for at opnå en fritagelse fra forbuddet om at videregive. Som minimum kan eksportøren eller den kompetente tilsynsmyndighed meddele den registrerede om suspenderingen eller ophøret af overførslen af vedkommendes personoplysninger, der skyldes importørens manglende evne til at overholde sine kontraktmæssige forpligtelser som følge af, at denne har modtaget en adgangsmodning.

126. Kontrakten kan forpligte eksportøren og importøren til at bistå den registrerede med at udøve vedkommendes rettigheder i tredjelandets jurisdiktion igennem ad hoc-erstatningsmekanismer og juridisk rådgivning.

127. Betingelser for effektivitet

- Nogle nationale lovgivninger tillader i givet fald ikke dataimportøren at yde registrerede denne form for bistand direkte, selv om de kan tillade, at dataimportøren tilvejebringer denne bistand til de registrerede.
- National lovgivning og nationale politikker kan pålægge betingelser, der kan undergrave effektiviteten af de fastlagte ad hoc-erstatningsmekanismer.
- Juridisk rådgivning kan være en hjælp for den registrerede, navnlig i betragtning af hvor komplekst og omkostningsfuldt det kan være for en registreret at forstå et tredjelandets retssystem og rejse søgsmål fra udlandet, der potentielt kan foregå på et fremmedsprog. Denne standardbestemmelse vil dog altid tilbyde en begrænset supplerende beskyttelse, da bistand og juridisk rådgivning til registrerede ikke alene kan afhjælpe mangler i et tredjelandets retsorden, som ikke kan sikre et beskyttelsesniveau, der reelt svarer til det, der er sikret inden for EØS. Denne kontraktmæssige foranstaltning vil derfor være nødt til at supplere andre supplerende foranstaltninger.
- Denne supplerende foranstaltning vil kun finde anvendelse, hvis tredjelandets lovgivning giver mulighed for klageprocedurer ved dets nationale domstole, eller hvis en ad hoc-erstatningsmekanisme forefindes, herunder mod overvågningsforanstaltninger.

2.3 Organisatoriske foranstaltninger

128. Yderligere organisatoriske foranstaltninger kan bestå af interne politikker, organisatoriske metoder og standarder, som dataansvarlige og databehandlere selv kan overholde og pålægge dataimportører i tredjelande. De kan bidrage til at sikre sammenhæng i beskyttelsen af personoplysninger under hele behandlingsforløbet. Organisatoriske foranstaltninger kan også forbedre eksportørernes bevidsthed om risici i forbindelse med og forsøg på at få adgang til dataene i tredjelande og deres kapacitet til at reagere på dem. Udvælgelse og gennemførelse af én eller flere af disse foranstaltninger vil ikke nødvendigvis og systematisk sikre, at jeres overførsel overholder standarden for væsentlig overensstemmelse, som krævet i EU-retten. Alt efter overførselens særlige omstændigheder og den vurdering, som er udført af tredjelandets lovgivning, er der brug for organisatoriske foranstaltninger til at supplere kontraktmæssige og/eller tekniske foranstaltninger for at sikre et niveau for beskyttelse af personoplysninger, der reelt svarer til det, der er sikret inden for EØS.
129. Vurderingen af de mest egnede foranstaltninger skal foretages fra sag til sag under hensyntagen til dataansvarliges og databehandlers behov for at overholde ansvarlighedsprincippet. Nedenfor angiver Databeskyttelsesrådet nogle eksempler på organisatoriske foranstaltninger, som eksportører kan implementere. Dog er listen ikke udtømmende, og andre foranstaltninger kan også være passende:

Interne politikker for forvaltning af overførsler, navnlig ved grupper af foretagender

130. Vedtagelse af passende interne politikker med tydelige fordelinger af ansvarsområder for dataoverførsler, rapporteringskanaler og standardprocedurer for tilfælde med formelle eller uformelle anmodninger fra offentlige myndigheder om at tilgå dataene. Navnlig i tilfælde af overførsler mellem grupper af foretagender kan disse politikker bl.a. omfatte udpegelsen af en særlig gruppe, som består af eksperter inden for IT, databeskyttelse og lovgivning om privatlivets fred, og som kan håndtere anmodninger, der involverer personoplysninger, der er overført fra EØS; notifikation af den overordnede juridiske ledelse og virksomhedsledelsen samt dataeksportøren ved modtagelsen af sådanne anmodninger; de proceduremæssige trin, der kan anfægte uforholdsmæssige eller ulovlige anmodninger, og levering af gennemsigtige oplysninger til registrerede.
131. Udviklingen af særlige uddannelsesprocedurer for personalet, der er ansvarligt for at behandle anmodninger om adgang til personoplysninger fra offentlige myndigheder, som bør ajourføres regelmæssigt for at afspejle nye udviklinger vedrørende lovgivning og retspraksis i tredjelandet og i EØS. Uddannelsesprocedurerne bør omfatte kravene i EU-retten vedrørende offentlige myndigheders adgang til personoplysninger, navnlig jf. artikel 52, stk. 1, i chartret om grundlæggende rettigheder. Personalets kendskab hertil bør øges, navnlig ved vurdering af praktiske eksempler på dataanmodninger fra offentlige myndigheder og ved at anvende standarden, som følger af artikel 52, stk. 1, i chartret om grundlæggende rettigheder, på sådanne praktiske eksempler. En sådan uddannelse bør tage hensyn til de særlige omstændigheder for dataimportøren, dvs. lovgivning og forskrifter i tredjelandet, som dataimportøren er underlagt, og bør udvikles i samarbejde med dataeksportøren, hvor det er muligt.

132. Betingelser for effektivitet:

- Disse politikker kan kun påtænkes i de tilfælde, hvor anmodningen fra offentlige myndigheder i tredjelandet er forenelig med EU-retten.¹⁰² Hvis anmodningen er uforenelig, vil disse politikker ikke være tilstrækkelige til at sikre et tilsvarende niveau for beskyttelse af personoplysninger, og, som nævnt i ovenstående, skal overførslerne standses, eller der skal fastlægges passende supplerende foranstaltninger for at undgå adgangen.

Foranstaltninger om gennemsigtighed og ansvarlighed

133. Dokumentér og registrér adgangsanmodningerne, som er modtaget fra offentlige myndigheder, og de leverede svar sammen med den juridiske begrundelse og de involverede aktører (f.eks. hvis eksportøren er blevet underrettet og dennes svar, vurderingen af holdet, som er ansvarligt for at behandle sådanne anmodninger, osv.). Disse dokumenter bør gøres tilgængelige for dataeksportøren, som derefter bør gøre dem tilgængelige for de berørte registrerede.

134. Betingelser for effektivitet:

- Tredjelandets nationale lovgivning kan forhindre offentliggørelsen af anmodningerne eller væsentlige oplysninger deri og dermed gøre denne praksis ineffektiv. Dataimportøren bør informere eksportøren om dennes manglende evne til at frembringe sådanne dokumenter og registre, hvilket dermed giver eksportøren mulighed for at suspendere overførslerne, hvis denne manglende evne ville føre til, at der ikke kan sikres et passende beskyttelsesniveau.

135. Regelmæssig offentliggørelse af gennemsigtighedsrapporter eller sammendrag vedrørende regeringers adgangsanmodninger og det svar, der er givet, hvis offentliggørelse tillades, jf. lokal lovgivning.

136. Betingelser for effektivitet:

- De leverede oplysninger bør være relevante, tydelige og så detaljerede som muligt. National lovgivning i tredjelandet kan forhindre offentliggørelse af detaljerede oplysninger. I de tilfælde bør dataeksportøren gøre sit bedste for at offentliggøre statistiske oplysninger eller lignende former for aggregerede oplysninger.

Organisatoriske metoder og foranstaltninger til dataminimering

137. Allerede eksisterende organisatoriske krav under ansvarlighedsprincippet, såsom vedtagelsen af streng og granulær dataadgang og fortrolighedspolitikker og bedste praksisser, der er baseret på et strengt need to know-princip, overvåget ved regelmæssige kontroller og håndhævet igennem en disciplinærordning, kan også være brugbare foranstaltninger i forbindelse med overførsler. Dataminimering bør overvejes i denne sammenhæng for at begrænse personoplysningers eksponering for uautoriseret adgang. I nogle tilfælde kan det for eksempel være nødvendigt at overføre visse data (f.eks. i tilfælde af fjernadgang til EØS-data, såsom i støttetilfælde, hvor

¹⁰² Jf. sag C-362/14 ("Schrems I"), præmis 94; C-311/18 (Schrems II), præmis 168, 174, 175 og 176.

begrænset adgang tildeles i stedet for fuld adgang, eller når leveringen af en tjeneste kun kræver overførslen af et begrænset datasæt og ikke en hel database).

138. Betingelser for effektivitet:

- Regelmæssige kontroller og en streng disciplinærordning bør være fastlagt for at overvåge og håndhæve overensstemmelse med foranstaltningerne til dataminimering (også i overførselssammenhænge).
- Dataeksportøren skal udføre en vurdering af personoplysningerne, denne besidder, inden overførslen finder sted, for at udpege de datasæt, som ikke er nødvendige til overførslen og derfor ikke deles med dataimportøren.
- Foranstaltninger til dataminimering bør ledsages af tekniske foranstaltninger for at sikre, at dataene ikke udsættes for uautoriseret adgang. For eksempel kan implementeringen af sikre flerparts beregningsmekanismer og spredning af krypterede datasæt blandt forskellige betroede enheder gennem design forhindre, at en unilateral adgang fører til offentliggørelse af identificerbare data.

139. Udvikling af bedste praksisser for på passende vis og rettidigt at involvere og give adgang til oplysninger til databeskyttelsesrådgiveren, hvis en sådan eksisterer, og til juridiske og interne revisionstjenester vedrørende emner, som er relateret til internationale overførsler af overførsler med personoplysninger.

140. Betingelser for effektivitet:

- Databeskyttelsesrådgiveren, hvis en sådan eksisterer, og det juridiske og interne revisionshold skal modtage alle relevante oplysninger inden overførslen og skal rådføres vedrørende overførselens nødvendighed og, i givet fald, yderligere garantier.
- Relevante oplysninger bør f.eks. omfatte en vurdering af nødvendigheden af at overføre de specifikke personoplysninger, et overblik over den gældende lovgivning i tredjelandet og de garantier, som importøren er forpligtet til at implementere.

Vedtagelse af standarder og bedste praksisser

141. Vedtagelse af strenge politikker om datasikkerhed og databeskyttelse, der er baseret på EU-certificeringer eller adfærdskodekser eller på internationale standarder (f.eks. ISO-standarder) og bedste praksisser (f.eks. ENISA) under hensyntagen til det aktuelle tekniske niveau i overensstemmelse med risikoen for de behandlede datakategorier.

Andet

142. Vedtagelse og regelmæssig gennemgang af interne politikker for at vurdere egnetheden af de implementerede supplerende foranstaltninger og udpegelse og implementering af yderligere eller alternative løsninger, om nødvendigt, for at sikre, at der opretholdes et beskyttelsesniveau for de overførte personoplysninger, der i det væsentlige svarer til det, der er sikret inden for EØS.

143. Forpligtelser fra dataimportøren om ikke at foretage nogen videreoverførsel af personoplysningerne inden for det samme eller andre tredjelande eller suspendere igangværende overførsler, når der i tredjelandet ikke kan sikres et beskyttelsesniveau for personoplysningerne, der i det væsentlige svarer til det, der er sikret inden for EØS.¹⁰³

¹⁰³ C-311/18 (Schrems II), præmis 135 og 137.

BILAG 3: MULIGE INFORMATIONSKILDER TIL VURDERING AF ET TREDJELAND

144. Jeres dataimportør bør være i stand til at forsyne jer med relevante kilder og informationer vedrørende tredjelandet, denne er etableret i, herunder den lovgivning og praksis, som er gældende for importøren og de overførte oplysninger. I og importøren kan finde oplysninger i flere informationskilder, f.eks. dem, der er anført i nedenstående ikke-udtømmende liste i prioriteret rækkefølge:

- Retspraksis fra Den Europæiske Unions Domstol (EU-Domstolen) og fra Den Europæiske Menneskerettighedsdomstol (EMD)¹⁰⁴ som angivet i henstillingen om europæiske væsentlige garantier¹⁰⁵
- Afgørelser om tilstrækkelighed i destinationslandet, hvis overførslen er baseret på et andet retsgrundlag¹⁰⁶
- Beslutninger og rapporter fra mellemstatslige organisationer, såsom Europarådet¹⁰⁷, andre regionale organer¹⁰⁸ og FN-organer og -agenturer (f.eks. FN's menneskerettighedsråd¹⁰⁹ og Menneskerettighedskomitéen¹¹⁰)
- Rapporter og analyser fra kompetente reguleringsnetværk, såsom Global Privacy Assembly (GPA);¹¹¹
- National retspraksis eller afgørelser truffet af uafhængige retlige eller administrative myndigheder, som er kompetente i forbindelse med datasikkerhed og databeskyttelse i tredjelande
- Rapporter fra uafhængige tilsynsorganer eller parlamentariske organer
- Rapporter baseret på praktiske erfaringer med tidligere tilfælde af anmodninger om offentliggørelse fra offentlige myndigheder eller fraværet af sådanne anmodninger, fra enheder inden for samme sektor som importøren
- "Warrant Canaries" fra andre enheder, der behandler oplysninger på samme område som importøren

¹⁰⁴ Se faktaarket for EMD's retspraksis vedrørende masseovervågning:

https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf

¹⁰⁵ Databeskyttelsesrådets henstilling nr. 02/2020 om europæiske væsentlige garantier for overvågningsforanstaltninger af 10. november 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en

¹⁰⁶ C-311/18 (Schrems II), præmis 141; se afgørelser om tilstrækkelighed i https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

¹⁰⁷ <https://www.coe.int/en/web/data-protection/reports-studies-and-opinions>

¹⁰⁸ Se f.eks. landerapporter fra Den Interamerikanske Kommission for Menneskerettigheder (IACHR), <https://www.oas.org/en/iachr/reports/country.asp>.

¹⁰⁹ Se <https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx>

¹¹⁰ Se:

https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=5

¹¹¹ Se f.eks. https://globalprivacyassembly.org/wp-content/uploads/2020/10/Day-1-1_2a-Day-3-3_2b-v1_0-Policy-Strategy-Working-Group-WS1-Global-frameworks-and-standards-Report-Final.pdf

- Rapporter udarbejdet eller bestilt af handelskamre, virksomheder, faglige sammenslutninger og brancheorganisationer, eksportørens statslige diplomatiske kontorer, handels- og investeringskontorer eller i andre tredjelande, der eksporterer til det tredjeland, hvortil overførslen foretages
- Rapporter fra akademiske institutioner og civilsamfundsorganisationer (f.eks. NGO'er).
- Rapporter fra private udbydere af business intelligence om finansielle, reguleringsmæssige og omdømmemæssige risici for virksomheder
- "Warrant Canaries" fra importøren selv¹¹²
- Gennemsigthedsrapporter, på betingelse af, at de udtrykkeligt nævner, at der ikke blev modtaget nogen anmodninger om adgang. Gennemsigthedsrapporter, der blot ikke nævner noget herom, anses ikke for at være tilstrækkelig dokumentation, da disse rapporter oftest har fokus på anmodninger om adgang modtaget fra retshåndhævende myndigheder og kun indeholder tal om dette aspekt, mens der ikke nævnes noget om anmodninger om adgang modtaget i forbindelse med formål vedrørende national sikkerhed. Dette betyder ikke, at der ikke blev modtaget nogen anmodninger om adgang, men snarere, at disse oplysninger ikke kan deles¹¹³
- Importørens interne optegnelser eller registre, hvoraf det udtrykkeligt fremgår, at der ikke blev modtaget nogen anmodninger i en tilstrækkelig lang periode, og fortrinsvis optegnelser og registre, som importøren er ansvarlig for og/eller er udarbejdet af personer i interne stillinger med en vis autonomi, såsom interne revisorer, databeskyttelsesrådgivere osv.¹¹⁴

¹¹² Se betingelser for at tage hensyn til importørens dokumenterede praktiske erfaringer med relevante tidligere tilfælde af anmodninger om adgang modtaget fra offentlige myndigheder i tredjelandet i punkt 47.

¹¹³ *Ibid.*

¹¹⁴ *Ibid.*