Vejledning om overførsel til tredjelande

Overførsel af personoplysninger til tredjelande

April 2024 (4. udgave)

DATATILSYNET

Indhold

Bilag 33

Baggrund

I dette indledende afsnit kan du læse om baggrunden for vejledningen, og hvordan vejledningen er opbygget.

Virksomheder og myndigheder kan have behov for at overføre personoplysninger til et land uden for EU/EØS[1] – et såkaldt tredjeland. Det kan eksempelvis være tilfældet, hvis man ønsker at udlicitere driften af IT-systemer eller at dele personoplysninger med en samarbejdspartner uden for EU/EØS.

I denne vejledning får du – som dataansvarlig eller databehandler – en kort introduktion til reglerne i databeskyttelsesforordningens kapitel V om overførsel af personoplysninger til tredjelande og internationale organisationer. Formålet med reglerne er overordnet at sikre, at den beskyttelse, som de registrerede borgere, kunder mv. er sikret efter databeskyttelsesforordningen, ikke bliver udvandet ved, at du overfører oplysningerne til lande eller organisationer uden for EU/EØS.

Bemærk i øvrigt, at der findes nogle særlige regler om overførsel af personoplysninger til tredjelande i retshåndhævelsesloven, som gælder for retshåndhævende myndigheder, dvs. politiet, anklagemyndigheden og kriminalforsorgen mv. Disse regler vil ikke blive gennemgået i denne vejledning.

Hvor finder jeg mere information?

Du kan læse mere om tredjelandsoverførsler på Datatilsynets hjemmeside.

Vejledningen er opbygget som et beslutningstræ, der skal guide dig godt igennem de overvejelser, der er relevante at gøre sig i forhold til tredjelandsoverførsler. Du kan finde en illustration (flowchart) af beslutningsprocessen som bilag 2 til denne vejledning. Hvis du allerede har erfaring med databeskyttelse og tredjelandsoverførsler, kan du med fordel springe direkte til **afsnit 4.**

Beslutningstræ:

Afsnit 1. Behandler jeg personoplysninger?
Afsnit 2. Overfører jeg personoplysninger til et tredjeland?
Afsnit 3. Hvor overfører jeg personoplysninger til?
Afsnit 4. Hvilke overførselsgrundlag kan jeg bruge til usikre tredjelande?
Afsnit 5. Hvad skal jeg i øvrigt være særligt opmærksom på?
Afsnit 6. Er der tale om en særlig situation?

1 EØS er forkortelsen for Det Europæiske Økonomiske Samarbejdsområde, som ud over EU-medlemsstaterne består af Norge, Island og Liechtenstein.

1. Behandler jeg personoplysninger?

Dette afsnit forklarer helt grundlæggende, hvad behandling af personoplysninger er.

Databeskyttelsesforordningens regler finder kun anvendelse, hvis du behandler personoplysninger. Det første helt grundlæggende spørgsmål, som du bør stille dig selv, er derfor, om du behandler personoplysninger.

Hvad er en personoplysning?

En personoplysning er enhver form for information, der kan henføres til en bestemt person, også selvom personen kun kan identificeres, hvis oplysningen kombineres med andre oplysninger.

Personoplysninger kan for eksempel være personnumre, registreringsnumre, et billede, en e-mailadresse, et telefonnummer, et fingeraftryk, en stemmeoptagelse, lægejournaler eller biologisk materiale, når det er muligt at identificere en person ud fra oplysningerne eller ved at sammenholde dem med andre personoplysninger. Man siger, at oplysningen er "personhenførbar".

Hvad er behandling af personoplysninger?

En behandling af personoplysninger kan have mange former. En behandling omfatter ifølge databeskyttelsesforordningen enhver håndtering af personoplysninger, herunder indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse.

Finder blot én af de nævnte former for håndtering af personoplysninger sted, vil der være tale om en behandling, som er omfattet af databeskyttelsesreglerne.

En behandling af personoplysninger kan således godt finde sted, selvom du ikke har læst eller aktivt anvendt de pågældende personoplysninger, f.eks. hvis du alene opbevarer personoplysningerne.

2. Overfører jeg personoplysninger til et tredjeland?

I dette afsnit kan du læse om, hvad en ”overførsel” er, herunder hvilke elementer du kan lægge vægt på, når du skal vurdere, om du overfører personoplysninger til et tredjeland.

Næste skridt er at undersøge, om den behandling af personoplysninger, som du foretager, indebærer en overførsel af personoplysninger til et tredjeland. Du skal med andre ord afklare, om du overfører personoplysninger ud af EU/EØS, og hvor du i givet fald overfører personoplysningerne til.

2.1 Hvad er en overførsel?

Databeskyttelsesforordningen indeholder ikke en definition af begrebet ”overførsel”. Begrebet er dog helt centralt for at kunne vurdere, hvornår du skal gøre brug af reglerne om overførsel til tredjelande i databeskyttelsesforordningens kapitel V.

Det Europæiske Databeskyttelsesråd har identificeret følgende tre kriterier, som alle skal være opfyldt for at kvalificere en behandlingsaktivitet som en overførsel:[2]

1) En dataansvarlig eller en databehandler ("dataeksportør") er omfattet af databeskyttelsesforordningen for den pågældende behandling.

2) Dataeksportøren videregiver eller stiller på anden måde personoplysninger, der er omfattet af denne behandling, til rådighed for en anden dataansvarlig, fælles dataansvarlig eller databehandler ("dataimportør").

3) Dataimportøren befinder sig i et tredjeland, uanset om denne dataimportør er omfattet af databeskyttelsesforordningen for den givne behandling,[3] eller er en international organisation.

Hvis de tre kriterier er opfyldt, er der tale om en overførsel omfattet af kapitel V i databeskyttelsesforordningen. Det betyder, at overførslen kun kan finde sted på visse betingelser, f.eks. på grundlag af en tilstrækkelighedsafgørelse fra Europa-Kommissionen (artikel 45) eller ved at give de fornødne garantier (artikel 46). Der findes dertil en række undtagelser til brug for særlige situationer (artikel 49). Bestemmelserne i kapitel V har til formål at sikre en fortsat beskyttelse af personoplysninger, efter de er blevet overført til et tredjeland eller en international organisation. Reglerne gælder for både myndigheder og private virksomheder.

Hvis de tre kriterier ikke er opfyldt, vil der ikke være tale om en overførsel, og kapitel V i forordningen finder ikke anvendelse. Man skal dog være opmærksom på, at den dataansvarlige stadig skal overholde de øvrige bestemmelser i databeskyttelsesforordningen og fortsat er fuldt ansvarlig for sine behandlingsaktiviteter, uanset hvor i verden de finder sted. Selvom en behandling af personoplysninger uden for EU/EØS ikke skal anses som en overførsel, kan behandlingen stadig være forbundet med øgede risici for de registrerede som følge af eksempelvis problematisk lovgivning eller uforholdsmæssig myndighedsadgang i tredjelandet. Den dataansvarlige skal tage højde for disse øgede risici, når der træffes foranstaltninger for at sikre, at behandlingen er i overensstemmelse med forordningen.

[2] Se afsnit 2 (s. 6ff) i EDPB’s Retningslinjer 05/2021 om samspillet mellem anvendelsen af artikel 3 og bestemmelserne om internationale overførsler i henhold til kapitel V i GDPR, udgave 2.0; vedtaget 14. februar 2023

[3] jf. databeskyttelsesforordningens artikel 3

På de næste sider er angivet en række eksempler på, hvordan begrebet ”overførsel” kan afgrænses nærmere i praksis.

Vejledninger

Retningslinjer 05/2021 om samspillet mellem anvendelsen af artikel 3 og bestemmelserne om internationale overførsler i henhold til kapitel V i GDPR

2.2 Situationer, der udgør en overførsel

Herunder finder du en række konkrete eksempler på situationer, hvor der er tale om en overførsel til et tredjeland:

Eksempel 1

Brug af cloud-løsning

Et forsikringsselskab i Danmark behandler oplysninger om sine kunder i et sagsbehandlingssystem. Sagsbehandlingssystemet er baseret på en cloud-løsning, hvor cloud-leverandøren befinder sig i Tyrkiet. Sagsbehandlingssystemet, herunder de personoplysninger, som behandles i systemet, bliver derfor lagret i et datacenter i Tyrkiet.

Når personoplysningerne lagres på en server hos cloud-leverandøren i Tyrkiet, sker der en overførsel, fordi personoplysningerne, som behandles af det danske forsikringsselskab (dataeksportøren), forlader EU/EØS og stilles til rådighed for cloudleverandøren i Tyrkiet (dataimportøren).

Eksempel 2

Outsourcing af IT-support

Et dansk teleselskab ønsker at benytte en virksomhed i Indien til IT-support, hvilket vil indebære behandling af personoplysninger. De indiske medarbejdere har ikke teknisk adgang til at lagre eller printe personoplysningerne hos den danske virksomhed, men har alene via en fjernadgang mulighed for at se oplysningerne, når de yder IT-support. Oplysningerne forlader således ikke EU/EØS.

Der er imidlertid tale om en overførsel til et tredjeland, fordi oplysningerne, som behandles af det danske teleselskab (dataeksportøren) gøres tilgængelige for supportmedarbejderne i virksomheden i Indien (dataimportøren). Det gør ingen forskel, at de indiske medarbejdere ikke forstår dansk, eller at de instrueres i ikke at søge i personoplysningerne.

Eksempel 3

Brug af konsulentservice

En konsulentvirksomhed i Danmark tilbyder en service, som går ud på at udarbejde statistik på baggrund af forbrugsvaner. En e-handelsplatform i Kina ønsker at gøre brug af denne service og sender til brug herfor oplysninger om sine kinesiske kunder til konsulentvirksomheden i Danmark.

Når virksomheden i Kina sender personoplysninger til virksomheden i Danmark, er der ikke tale om en overførsel til et tredjeland, da oplysningerne overføres fra Kina til Danmark. Hvis personoplysningerne efter endt behandling hos den danske virksomhed (dataeksportøren) returneres til virksomheden i Kina (dataimportøren), vil dette imidlertid være en overførsel, fordi personoplysningerne forlader EU/EØS og stilles til rådighed for en virksomhed i et tredjeland. Det har i den forbindelse ingen betydning, at der er tale om oplysninger om kinesiske personer, som fysisk befinder sig uden for EU/EØS.

Eksempel 4

Vedligeholdelse og fejlretning af cloud-løsning

En dansk virksomhed anvender en cloud-løsning til databehandling, herunder dokumentdeling, videokonferencer og afsendelse af e-mails. Brugen af denne service indebærer behandling af personoplysninger. Personoplysningerne bliver som udgangspunkt lagret i et datacenter i Tyskland. Da løsningen er meget kompleks, er der dog jævnligt behov for, at udbyderen af cloud-løsningen foretager fejlretning og vedligeholdelse af løsningen. Dette udføres fra Ukraine, hvor cloud-udbyderen er etableret.

Hvis cloud-udbyderen i Ukraine i forbindelse med fejlretning og vedligeholdelse af cloud-løsningen får adgang til personoplysninger, som behandles af den danske virksomhed, vil der i disse tilfælde være tale om en overførsel af personoplysninger fra den danske virksomhed (dataeksportøren) til den ukrainske cloud-udbyder (dataimportøren).

Eksempel 5

Brug af nyhedsbrevsservice

En dansk modevirksomheds kunder kan skrive sig op til at modtage et nyhedsbrev fra virksomheden. Modevirksomheden benytter en virksomhed i Chile til at udsende nyhedsbrevet og sender derfor e-mailadresser på de kunder, som skal modtage nyhedsbrevet, til virksomheden i Chile.

Når modevirksomheden (dataeksportøren) sender e-mailadresser på sine kunder til virksomheden i Chile (dataimportøren), er der tale om en overførsel af personoplysninger til et tredjeland, idet oplysningerne forlader EU/EØS og stilles til rådighed for den chilenske virksomhed.

Eksempel 6

Brug af chat- og kundeservicefunktion

En møbelvirksomhed i Danmark gør brug af en IT-løsning bestående af en chat- og kundeservicefunktion, som gør det muligt for møbelvirksomheden at hjælpe kunder med spørgsmål om produkter mv. i virksomhedens webshop. Kommunikationen vil typisk inkludere personoplysninger i form af kundernes e-mailadresser, navne og historik i forhold til eventuelle tidligere henvendelser.

IT-løsningen er cloud-baseret og bliver udbudt af en leverandør, som er etableret i USA. Når løsningen benyttes, lagres al kommunikation mellem møbelvirksomheden og kunderne, herunder deres personoplysninger, på cloud-leverandørens servere i USA. Når kunderne benytter chat- og kundeservicefunktionen hos den danske møbelvirksomhed (dataeksportøren), sker der således en overførsel af deres personoplysninger, idet oplysningerne lagres hos – og dermed stilles til rådighed for - cloudleverandøren (dataimportøren) i USA.

Eksempel 7

Adgang til oplysninger hos koncernrelaterede virksomheder

En dansk virksomhed udstationerer medarbejdere i en virksomhed i Singapore. Virksomhederne i Danmark og Singapore er del af samme koncern. Medarbejdernes arbejdstilladelse, kontrakt og billede af pas bliver gemt på en server placeret hos virksomheden i Danmark. Virksomheden i Singapore har efter behov adgang til at hente disse data fra serveren i Danmark, f.eks. hvis myndighederne i Singapore stiller krav om det i henhold til national lovgivning.

Når virksomheden i Singapore henter de pågældende oplysninger, sker der en overførsel af personoplysninger, idet oplysningerne forlader den danske virksomhed (dataeksportøren) og stilles til rådighed for virksomheden i Singapore (dataimportøren).

Selvom de to virksomheder tilhører samme koncern, er der tale om to forskellige enheder, som i dette tilfælde hver især er dataansvarlige for deres behandling af personoplysningerne. og der er derfor tale om en overførsel af personoplysninger (modsat eksempel 8 og 9 i næste afsnit, hvor personoplysningerne ikke overføres til en anden dataansvarlig eller databehandler).

2.3 Situationer, der ikke udgør en overførsel

Herunder finder du en række konkrete eksempler på situationer, hvor der ikke er tale om en overførsel til et tredjeland:

Eksempel 8

Forretningsrejse

En dansk IT-leverandør ønsker at indgå en aftale med en pakistansk virksomhed om salg af en IT-løsning.

I den forbindelse rejser to af IT-leverandørens medarbejdere til Pakistan for at præsentere virksomhedens produkt for den pakistanske virksomhed. Med sig har de deres arbejdscomputere, der kan kobles på virksomhedens netværk hjemme i Danmark.

Når de to medarbejdere under opholdet i Pakistan logger på den danske virksomheds netværk og tilgår e-mails mv., som indeholder personoplysninger, vil der ikke være tale om en overførsel til et tredjeland, fordi medarbejderne er en del af virksomheden og ikke skal anses som selvstændige dataansvarlige eller databehandlere i forhold til deres arbejdsgiver. Den danske IT-leverandør er således stadig dataansvarlig for sine ansattes (arbejdsrelaterede) behandling af personoplysninger, mens de opholder sig i Pakistan.

Hvis medarbejderne derimod overlader personoplysningerne til den pakistanske virksomhed, vil der være tale om en overførsel, fordi oplysningerne af den danske virksomhed stilles til rådighed for en anden dataansvarlig eller databehandler i et tredjeland.

Selvom databeskyttelsesforordningens regler om overførsel til tredjelande ikke finder anvendelse i eksemplet, skal IT-leverandøren stadigvæk som dataansvarlig sikre overholdelse af databeskyttelsesforordningens øvrige regler – herunder reglerne om behandlingssikkerhed – når medarbejderne behandler personoplysninger i et tredjeland. Det betyder i praksis, at medarbejderne ikke kan behandle personoplysninger under deres forretningsrejse, hvis IT-leverandøren ikke er i stand til at sikre databeskyttelsesforordningens fulde overholdelse ved hjælp af enten organisatoriske eller tekniske foranstaltninger.

Eksempel 9

Kontor i tredjeland

En dansk virksomhed har et internationalt kontor i Ægypten. For at medarbejderne på kontoret kan varetage deres arbejde, har de brug for at tilgå virksomhedens systemer i Danmark fra kontoret i Ægypten.

Der vil ikke være tale om en overførsel til et tredjeland, idet kontoret godt nok geografisk befinder sig uden for EU/EØS, men ikke er en selvstændig dataansvarlig eller databehandler i forhold til den danske virksomhed. Medarbejdernes nationalitet har ingen betydning for denne vurdering. De er ansat i den danske virksomhed, som er dataansvarlig for sine medarbejderes behandling af personoplysninger.

Dette vil også gøre sig gældende i andre lignende situationer. Det gælder f.eks. når en medarbejder udstationeres i et tredjeland eller ansættes med fast hjemmearbejdsplads i et tredjeland, hvor medarbejderen er bosiddende, forudsat at der ikke er tale om, at medarbejderen er selvstændig dataansvarlig eller databehandler.

Hvis kontoret i stedet var en selvstændig dataansvarlig eller databehandler, f.eks. et datterselskab i en koncern, ville der være tale om en overførsel til et tredjeland, hvis kontoret havde adgang til personoplysninger hos den danske virksomhed.

Selvom databeskyttelsesforordningens regler om overførsel til tredjelande ikke finder anvendelse i en situation som den ovenfor beskrevne, påhviler det den dataansvarlige virksomhed at sikre overholdelse af alle databeskyttelsesforordningens regler. Det betyder, at virksomheden – hvis den ikke kan sikre databeskyttelsesforordningens fulde overholdelse ved hjælp af organisatoriske eller tekniske foranstaltninger – ikke vil kunne behandle oplysningerne på det pågældende kontor.

Eksempel 10

Særligt om udlevering af personoplysninger efter anmodning fra myndigheder i tredjelande

En databehandler må kun behandle personoplysninger, herunder overføre oplysningerne til tredjelande, i det omfang den dataansvarlige har givet instruktioner om det i databehandleraftalen, eller det er krævet ifølge EU-ret eller medlemsstaternes nationale ret.

Hvis en databehandler i EU/EØS også er etableret i et tredjeland, kan databehandleren dog i nogle tilfælde blive mødt af en anmodning fra myndighederne i dette tredjeland om udlevering af personoplysninger, som databehandleren behandler for den dataansvarlige.

Hvis databehandleren vælger at overføre personoplysninger til tredjelandet i strid med databehandleraftalen, vil der være tale om en utilsigtet overførsel, og det betyder, at databeskyttelsesforordningens regler om overførsel til tredjelande ikke finder anvendelse i forhold til den dataansvarlige.

Den dataansvarlige skal dog være opmærksom på en række forhold i den forbindelse:

For det første må den dataansvarlige kun benytte databehandlere, som kan stille de fornødne garantier for, at databeskyttelsesforordningens regler bliver overholdt. I den forbindelse bør den dataansvarlige anmode databehandleren om tydeligt at tilkendegive, om denne er underlagt lovgivning i tredjelandet, som - på trods af den dataansvarliges instruks om det modsatte - pålægger databehandleren at udlevere personoplysninger, som befinder sig i EU/EØS, til tredjelandets myndigheder. Hvis den dataansvarlige bliver bekendt med, at databehandleren er underlagt sådan lovgivning, skal den dataansvarlige ophøre med at benytte databehandleren.

For det andet skal den dataansvarlige sikre den nødvendige behandlingssikkerhed, herunder at databehandleren behandler personoplysningerne fortroligt og ikke gør dem tilgængelige for uvedkommende. Den dataansvarlige må i den forbindelse foretage en risikovurdering med henblik på at vurdere, hvilke tiltag der skal iværksættes for at sikre dette.

For det tredje skal den dataansvarlige føre tilsyn med sin databehandler. Hvis den dataansvarlige bliver bekendt med, at databehandleren handler i strid med databehandleraftalen ved at overføre personoplysninger til et tredjeland mod den dataansvarliges instruks, skal den dataansvarlige straks gribe ind over for dette.

Det bemærkes i øvrigt, at hvis en databehandler handler i strid med databehandleraftalen ved at videregive personoplysninger til en myndighed i et tredjeland og dermed selv fastlægger formålene med og hjælpemidlerne til en behandling, vil denne blive anset for selvstændig dataansvarlig for den pågældende behandling og dermed omfattet af reglerne i kapitel V, for så vidt angår den konkrete overførsel.

3. Hvor overfører jeg personoplysninger til?

I dette afsnit kan du læse om de forskellige typer af tredjelande eller internationale organisationer, og hvad dette betyder for dig som dataeksportør.

I de følgende afsnit beskrives det nærmere, hvordan du skal forholde dig ved overførsel af personoplysninger til de forskellige typer af tredjelande eller internationale organisationer.

3.1 EU- og EØS-lande

Hvis den behandling af personoplysninger, som du foretager, indebærer transmission af personoplysninger til et andet EU-land eller et EØS-land (Island, Liechtenstein og Norge), finder reglerne i databeskyttelsesforordningen om overførsler ikke anvendelse.

3.2 Sikre tredjelande

Databeskyttelsesforordningens artikel 45 giver mulighed for, at Europa-Kommissionen kan træffe en såkaldt tilstrækkelighedsafgørelse, hvis beskyttelsesniveauet for personoplysninger i et tredjeland eller en international organisation i det væsentlige svarer til beskyttelsesniveauet i EU/EØS. I daglig tale kaldes lande omfattet af en tilstrækkelighedsafgørelse "sikre tredjelande".

Ved sin vurdering analyserer Europa-Kommissionen bl.a. de regler, der gælder for behandling af personoplysninger i tredjelandet, og hvordan tredjelandet efterlever grundlæggende retsstatsprincipper, herunder sikrer de registreredes ret til klageadgang og domstolsprøvelse, mv.

En overførsel til sikre tredjelande eller organisationer kan som udgangspunkt ske uden videre, alene på grundlag af tilstrækkelighedsafgørelsen, hvorimod en overførsel til usikre tredjelande eller organisationer kræver, at dataeksportøren giver fornødne garantier for at sikre en fortsat beskyttelse af de overførte oplysninger, eller at nogle særlige undtagelser finder anvendelse.

Hvis du ønsker at overføre personoplysninger til et tredjeland, bør du derfor som det første skridt undersøge, om Europa-Kommissionen har truffet en tilstrækkelighedsafgørelse for det pågældende land.

Selvom et land benævnes "sikkert tredjeland", skal du være opmærksom på, at Europa-Kommissionens tilstrækkelighedsafgørelse ikke altid dækker hele landet. Tilstrækkelighedsafgørelsen kan nemlig være begrænset til at vedrøre et bestemt område eller én eller flere sektorer i det pågældende tredjeland.

Europa-Kommissionen foretager regelmæssige evalueringer af tilstrækkelighedsafgørelserne og kan i den forbindelse finde behov for at ændre, ophæve eller erstatte en tilstrækkelighedsafgørelse, hvis forholdene i det pågældende land har ændret sig. Det kan betyde, at tredjelande, som Europa-Kommissionen tidligere har vurderet som sikre, ikke længere kan opretholde denne status. Du bør derfor altid orientere dig på Europa-Kommissionens hjemmeside for at få en opdateret liste over sikre tredjelande. [4]

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

Nedenfor i figur 1 og 2 finder du en liste over de tredjelande eller områder/sektorer i tredjelande, som Europa-Kommissionen på tidspunktet for denne vejlednings udarbejdelse har vurderet som værende sikre. For eventuelle senere opdateringer henvises til Europa-Kommissionens hjemmeside.

Figur 1

OVERSIGT OVER SIKRE TREDJELANDE		
Andorra	**Argentina**	**Guernsey**
Isle of Man	**Israel**	**Jersey**
New Zealand	**Schweiz**	**Storbritannien**
Sydkorea	**Uruguay**	

Figur 1

OVERSIGT OVER SIKRE OMRÅDER/SEKTORER I TREDJELANDE	
Canada	Gælder modtagere omfattet af den canadiske Personal Information Protection and Electronic Documents Act (PIPEDA).[5]
Færøerne	Gælder modtagere, der er omfattet af den færøske lov om behandling af personoplysninger. Overførsler til rigsmyndighederne, dvs. eksempelvis Rigsombudsmanden, Retten på Færøerne, Færøernes Politi, Kriminalforsorgen på Færøerne mv., er ikke omfattet.[6]
Japan	Gælder modtagere omfattet af den japanske Act on the Protection of Personal Information (APPI).[7]
USA	Gælder modtagere, der har certificeret sig under EU-U.S. Data Privacy Framework hos det amerikanske handelsministerium (Department of Commerce).[8]

[5] Du kan læse mere om PIPEDA her

[6] En engelsk oversættelse af den færøske lov om behandling af personoplysninger er tilgængelig her

[7] En engelsk oversættelse af APPI er tilgængelig her

[8] Se den aktuelle liste over certificerede virksomheder her

3.3 Usikre tredjelande

Et tredjeland betegnes som "usikkert", hvis Europa-Kommissionen ikke har truffet en tilstrækkelighedsafgørelse som omtalt ovenfor i afsnit 3.2. Hvis du ønsker at overføre personoplysninger til et usikkert tredjeland, skal du selv give de fornødne garantier for en tilstrækkelig beskyttelse af de overførte oplysninger ved at bruge et af overførselsgrundlagene i databeskyttelsesforordningens artikel 46. Disse er beskrevet nedenfor i afsnit 4. I helt særlige situationer og under en række betingelser kan man anvende en af undtagelserne i artikel 49, som er beskrevet i afsnit 6.

Særligt om Rigsfællesskabet - Færøerne og Grønland

Selvom Færøerne og Grønland er en del af Rigsfællesskabet, er de i databeskyttelsesretlig forstand at betragte som tredjelande.

Europa-Kommissionen har truffet en tilstrækkelighedsafgørelse vedrørende Færøerne, som dermed er et sikkert tredjeland. Du skal dog være opmærksom på, at rigsmyndighederne (f.eks. politiet, kriminalforsorgen og Rigsombudsmanden) ikke er omfattet af tilstrækkelighedsafgørelsen. Du skal derfor have et overførselsgrundlag i artikel 46 eller kunne identificere en relevant undtagelse i artikel 49, hvis du vil overføre personoplysninger til disse myndigheder.

Europa-Kommissionen har ikke truffet en tilstrækkelighedsafgørelse vedrørende Grønland, som derfor er et usikkert tredjeland. Hvis du ønsker at overføre personoplysninger til Grønland, skal du sørge for at have et overførselsgrundlag i artikel 46 eller kunne identificere en relevant undtagelse i artikel 49.

3.4 Internationale organisationer

Hvis en international organisation ikke er omfattet af databeskyttelsesforordningens regler, skal du betragte den på samme måde som et tredjeland, hvilket betyder, at du som udgangspunkt skal have et overførselsgrundlag, når du overfører personoplysninger til en sådan organisation.[9] En international organisation kan f.eks. være FN eller OECD.

Det betyder også, at Europa-Kommissionen kan træffe en tilstrækkelighedsafgørelse, som vil indebære, at den pågældende internationale organisation betragtes som sikker, og at der kan overføres personoplysninger til organisationen på grundlag af tilstrækkelighedsafgørelsen.

Europa-Kommissionen har på tidspunktet for denne vejlednings udarbejdelse ikke truffet tilstrækkelighedsafgørelser i relation til internationale organisationer, men du kan holde dig opdateret herom på Europa-Kommissionens hjemmeside[10].

[9] At en international organisation ikke er omfattet af databeskyttelsesforordningens regler kan f.eks. skyldes regler om immunitet.

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

4. Hvilke overførselsgrundlag kan jeg bruge til usikre tredjelande?

I dette afsnit kan du læse om de forskellige overførselsgrundlag i databeskyttelsesforordningens artikel 46.

Hvis du overfører personoplysninger til et tredjeland, som Europa-Kommissionen ikke har vurderet til at have et tilstrækkeligt beskyttelsesniveau, er der tale om en overførsel til et "usikkert tredjeland".

I disse situationer kan du som udgangspunkt kun overføre personoplysninger til tredjelandet, hvis du kan give de fornødne garantier for, at beskyttelsesniveauet for de overførte oplysninger i det væsentlige svarer til dét inden for EU/EØS. Dette kræver i første omgang et overførselsgrundlag i databeskyttelsesforordningens artikel 46. Dertil kan der afhængig af forholdene i modtagerlandet konkret være behov for supplerende foranstaltninger for at sikre en tilstrækkelig beskyttelse, som nærmere beskrevet nedenfor i afsnit 5.1.

Ved vurderingen af, hvilket overførselsgrundlag, der passer bedst til din organisation, har det bl.a. betydning, om du er en privat virksomhed eller en offentlig myndighed, om din virksomhed indgår i en større koncern, hvor hurtigt du skal bruge overførselsgrundlaget, mv. Du skal også være opmærksom på, at der er forskel på de garantier, du skal give, alt efter om du er dataansvarlig eller databehandler.

I afsnit 4.1-4.6 kan du læse mere om de forskellige overførselsgrundlag i artikel 46, og i skemaet nedenfor finder du et overblik over målgruppe samt fordele og ulemper for de respektive overførselsgrundlag (Skemaet er også vedlagt som bilag 1).

Figur 4

Overførselsgrundlag	Målgruppe	Ulemper	Fordele
Standardbestemmelser *Art. 46, stk. 2, litra c) og d)*	• Offentlige myndigheder og private virksomheder	• Begrænset mulighed for at foretage ændringer	• Intet krav om godkendelse fra Datatilsynet • Kan anvendes i de fleste overførselssituationer • Moduler kan kombineres, så én aftale kan dække flere overførselssituationer • Der kan løbende tilføjes/fjernes parter • Kan indgå i databehandleraftalen eller hovedaftalen, så man kan nøjes med ét samlet aftaledokument
Ad hoc-kontrakter *Art. 46, stk. 3, litra a)*	• Offentlige myndigheder og private virksomheder	• Skal godkendes af Datatilsynet og EDPB • Kan være ressourcekrævende at udarbejde	• Anvendes typisk som alternativ til standardbestemmelserne • Du har selv indflydelse på indhold og udformning og kan skræddersy kontrakten til den specifikke overførselssituation
Bindende virksomhedsregler *Art. 47, jf. art. 46, stk. 2, litra b)*	• Større koncerner og grupper af foretagender, der udøver en fælles økonomisk aktivitet	• Skal godkendes af Datatilsynet og EDPB • Kan være ressourcekrævende at udarbejde • Kan kun anvendes internt i koncernen	• Kan dække alle overførsler indenfor en koncern • Kan indgå som en del af koncernens samlede compliance-opsætning
Retligt bindende instrument *Art. 46, stk. 2, litra a)*	• Offentlige myndigheder • Private virksomheder, hvis dette fremgår af det retligt bindende instrument	• Kan være ressourcekrævende at udarbejde	• Intet krav om godkendelse fra Datatilsynet • Kan dække alle overførsler omfattet af det retligt bindende instrument
Administrative ordninger *Art. 46, stk. 3, litra b)*	• Offentlige myndigheder	• Skal godkendes af Datatilsynet og EDPB	• Kan dække alle overførsler mellem de involverede myndigheder
Adfærdskodekser *Art. 46, stk. 2, litra e)*	• Offentlige myndigheder og private virksomheder	• Endnu ingen godkendte adfærdskodekser til brug for overførsler	• Kan dække alle overførsler til en dataimportør, som har tilsluttet sig et godkendt adfærdskodeks
Certificeringsordninger *Art. 46, stk. 2, litra f)*	• Offentlige myndigheder og private virksomheder	• Endnu ingen godkendte certificeringsordninger til brug for overførsler	• Kan dække alle overførsler til en certificeret dataimportør

4.1 Standardbestemmelser om databeskyttelse

Et af de mest anvendte overførselsgrundlag er Europa-Kommissionens standardbestemmelser - også kaldet standardkontrakter eller SCC (standard contractual clauses) - der fungerer som en skabelon, der udfyldes og underskrives af dataeksportøren og dataimportøren. Både Europa-Kommissionen og de nationale tilsynsmyndigheder har mulighed for at vedtage sådanne standardbestemmelser til brug for overførsler, men indtil videre er det kun Europa-Kommissionen, der har udnyttet muligheden.

Standardbestemmelserne har et bredt anvendelsesområde og kan således anvendes ved overførsel af personoplysninger til tredjelande både mellem myndigheder og virksomheder, herunder i og uden for koncernforhold. Hvis der foreligger et koncernforhold, kan det dog være mere oplagt at anvende bindende virksomhedsregler (BCR) som overførselsgrundlag, som beskrevet i afsnit 4.3 nedenfor.

Europa-Kommissionen vedtog den 4. juni 2021 de gældende standardbestemmelser til brug for overførsel til tredjelande.[11] Standardbestemmelserne består af flere særskilte moduler, som skal kombineres alt efter, hvilken overførselssituation man befinder sig i. Det er muligt at benytte de nye standardbestemmelser i følgende fire overførselssituationer:

- Modul 1: Overførsel fra dataansvarlig til dataansvarlig
- Modul 2: Overførsel fra dataansvarlig til databehandler
- Modul 3: Overførsel fra databehandler til (under-)databehandler
- Modul 4: Overførsel fra databehandler til dataansvarlig

Hvis du ønsker at benytte standardbestemmelser som overførselsgrundlag, skal du ikke have en forudgående godkendelse fra Datatilsynet. Du bør dog altid sikre dig, at du som dataeksportør har anvendt standardbestemmelserne korrekt, og at du og dataimportøren i øvrigt er i stand til at leve op til de forpligtelser, der følger af standardbestemmelserne.

Standardbestemmelserne indeholder en såkaldt "docking clause", som gør det muligt løbende at udskifte eller tilføje parter til aftalen, hvilket særligt kan være relevant ved mere komplekse behandlingsaktiviteter.

Du kan derudover lade standardbestemmelserne indgå som en del af en bredere kontrakt mellem dig og dataimportøren samt tilføje andre klausuler eller yderligere garantier, forudsat at de ikke direkte eller indirekte er i strid med standardbestemmelserne. Det vil eksempelvis være muligt at inkludere bestemmelser om anvendelse af supplerende foranstaltninger, uden at det kræver en godkendelse fra Datatilsynet. For så vidt angår overførsler fra dataansvarlige til databehandlere eller fra databehandlere til (under-)databehandlere (modul 2 og 3), inkorporerer standardbestemmelserne kravene efter forordningens artikel 28. Du behøver dermed ikke indgå en separat databehandleraftale med din dataimportør ved siden af aftalen om overførslen.

Hvis du ændrer i standardbestemmelserne i strid med deres indhold, skal du være opmærksom på, at de hermed vil ændre karakter og blive til en såkaldt ad hoc-kontrakt, som kræver godkendelse fra Datatilsynet. Se mere herom i afsnit 4.2 nedenfor.

Du kan læse mere om, hvordan man anvender standardbestemmelserne, i Europa-Kommissionens FAQ.[12]

4.2 Ad hoc-kontrakter

En ad hoc-kontrakt er et dokument, der sprogligt og formmæssigt har et andet indhold end de standardbestemmelser om databeskyttelse, der er vedtaget af Europa-Kommissionen eller af en tilsynsmyndighed, jf. afsnit 4.1 ovenfor. Fordelen ved at benytte en ad hoc-kontrakt er, at du får mulighed for selv at tilpasse indholdet af kontrakten til den konkrete situation. Det kan

[11] Kommissionens Gennemførelsesafgørelse (EU) 2021/914 af 4. juni 2021 om standardkontraktbestemmelser for overførsel af personoplysninger til tredjelande i henhold til Europa-Parlamentets og Rådets forordning (EU) 2016/679

[12] New Standard Contractual Clauses - Questions and Answers overview (europa.eu)

således være relevant at bruge en ad hoc-kontrakt, hvis ingen af de eksisterende standardbestemmelser passer på den konkrete overførselssituation.

En ulempe ved at benytte ad hoc-kontrakter er dog, at de skal godkendes af Datatilsynet, der er forpligtet til at indhente en udtalelse fra Det Europæiske Databeskyttelsesråd. Denne procedure tager tid, og Datatilsynet anbefaler derfor, at man så vidt muligt anvender Europa-Kommissionens standardbestemmelser.

Ønsker du alligevel at udarbejde en ad hoc-kontrakt, kan du med fordel tage udgangspunkt i Europa-Kommissionens standardbestemmelser, da ad hoc-kontrakter vil skulle indeholde mange af de samme elementer for at kunne godkendes.

Du kan både som dataansvarlig og databehandler ansøge om Datatilsynets godkendelse af en ad hoc-kontrakt. Generelt er det dog den dataansvarlige, som har det overordnede ansvar for at sikre, at en behandling lever op til databeskyttelsesforordningens regler, herunder at der sikres et gyldigt overførselsgrundlag ved overførsel af personoplysninger til tredjelande.

4.3 Bindende virksomhedsregler (BCR)

Hvis din virksomhed er en del af en større koncern eller en gruppe af foretagender, som udøver en fælles økonomisk aktivitet, med tilstedeværelse i flere usikre tredjelande, kan du anvende bindende virksomhedsregler – ofte også kaldet BCR (Binding Corporate Rules) – som overførselsgrundlag. Bindende virksomhedsregler kan dog kun anvendes, når du overfører personoplysninger internt mellem koncernens virksomheder eller gruppens medlemmer. Der findes bindende virksomhedsregler til dataansvarlige (BCR-C) og til databehandlere (BCR-P).

Figur 5

Fordelen ved at benytte bindende virksomhedsregler er, at du som f.eks. europæisk virksomhed i en multinational koncern ikke skal sørge for et separat overførselsgrundlag, hver gang du overfører personoplysninger til koncernens virksomheder uden for EU/EØS. Dertil kan de bindende virksomhedsregler indarbejdes i koncernens eksisterende forretningsgange, politikker og kontrolprocedurer og fungere som en global databeskyttelsespolitik for hele koncernen.

Du skal være opmærksom på, at bindende virksomhedsregler skal godkendes af Datatilsynet. Dette er en længere proces, da andre europæiske datatilsynsmyndigheder og i sidste ende Det Europæiske Databeskyttelsesråd også skal inddrages i den særlige godkendelsesprocedure.

Du kan læse mere på Datatilsynets hjemmeside om ansøgningsprocessen og hvilke krav de bindende virksomhedsregler skal opfylde. Du kan også læse nærmere om den forventede sagsbehandlingstid for endelig godkendelse af dine bindende virksomhedsregler.[13]

Vejledninger

- EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR)
- WP 257 – Arbejdsdokument om tjekliste over de elementer og principper, som skal være indeholdt i bindende virksomhedsregler for databehandlere*
- WP 265 - Anbefaling om standardansøgning til brug for godkendelse af bindende virksomhedsregler for databehandlere*

**EDPB er i færd med at opdatere WP257 og WP265.*

4.4 Retligt bindende instrumenter mellem offentlige myndigheder eller organer

En offentlig myndighed kan overføre personoplysninger til en anden offentlig myndighed i et tredjeland på baggrund af et såkaldt retligt bindende instrument. Et sådant instrument kan eksempelvis være en international traktat eller konvention, som er retligt bindende og dermed kan håndhæves i tredjelandet. En international aftale kan efter omstændighederne også anvendes som overførselsgrundlag af private parter, såfremt aftalen fastsætter dette.

Det er vigtigt, at du fastslår, om instrumentet er retligt bindende eller ej. Det vil sige, om parterne kan håndhæve instrumentet over for hinanden. Hvis instrumentet er retligt bindende, skal du nemlig ikke ansøge om godkendelse af instrumentet hos Datatilsynet, inden det kan tages i brug.

Det Europæiske Databeskyttelsesråd har udarbejdet anbefalinger, som skal sikre, at retligt bindende instrumenter mellem offentlige myndigheder er i overensstemmelse med databeskyttelsesforordningens regler. I den forbindelse har Det Europæiske Databeskyttelsesråd også udarbejdet en liste over de garantier, der som minimum skal medtages i instrumentet.

4.5 Bestemmelser i administrative ordninger mellem offentlige myndigheder

Hvis du er en offentlig myndighed, kan du overføre personoplysninger til en anden offentlig myndighed i et tredjeland på baggrund af bestemmelser i en administrativ ordning, som indeholder effektive rettigheder, der kan håndhæves, for de registrerede. Det kan eksempelvis være et aftalememorandum (Memorandum of Understanding), hvorved parterne tilkendegiver en fælles intention om at samarbejde, uden at parterne er retligt forpligtede hertil.

Det er et krav, at ordningen sikrer rettigheder for de registrerede, som kan håndhæves.

Det Europæiske Databeskyttelsesråd har udarbejdet anbefalinger, som skal sikre, at administrative ordninger mellem offentlige myndigheder er i overensstemmelse med databeskyttelsesforordningens regler. I den forbindelse har Det Europæiske Databeskyttelsesråd også udarbejdet en liste over de garantier, der som minimum skal medtages i instrumentet.

13 https://www.datatilsynet.dk/internationalt/tredjelandsoverfoersler

Når der er tale om administrative ordninger, som ikke er juridisk bindende, er det nødvendigt at få en godkendelse fra Datatilsynet, hvilket oftest også vil kræve inddragelse af Det Europæiske Databeskyttelsesråd.

Vejledninger

Retningslinjer 2/2020 om artikel 46, stk. 2, litra a), og artikel 46, stk. 3, litra b), i forordning (EF) nr. 2016/679 om overførsel af personoplysninger mellem myndigheder i EØS og offentlige myndigheder og organer uden for EØS

4.6 Adfærdskodekser og certificeringsmekanismer til brug for overførsler

Der er endnu ikke godkendt adfærdskodekser eller certificeringsmekanismer til brug for overførsler til tredjelande fra EU/EØS.

Adfærdskodekser og certificeringsmekanismer kan dog på sigt være interessante at benytte som overførselsgrundlag af især små og mellemstore virksomheder. Det skyldes bl.a., at det ikke er dig som dataeksportør, som er ansvarlig for at udarbejde – og få godkendt – adfærdskodeksen eller certificeringsmekanismen. Det vil ofte være brancheorganisationer eller andre større sammenslutninger, som udarbejder adfærdskodekser eller certificeringsordninger inden for en bestemt branche eller sektor med henblik på at gøre det lettere for aktører på området at overholde databeskyttelsesforordningens regler. Også her er der tale om en længere godkendelsesprocedure med inddragelse af bl.a. Det Europæiske Databeskyttelsesråd.

Hvis en virksomhed i et tredjeland tilslutter sig en godkendt adfærdskodeks eller certificeringsordning til brug for overførsler, vil du som dataeksportør i EU/EØS kunne overføre personoplysninger til virksomheden på dette grundlag, og du behøver ikke en forudgående godkendelse fra Datatilsynet.

Du skal være opmærksom på, at der også findes adfærdskodekser og certificeringsordninger, som er vedtaget med henblik på at bidrage til korrekt anvendelse af databeskyttelsesforordningen og til at påvise, at dataansvarliges og databehandleres behandlingsaktiviteter overholder databeskyttelsesforordningen.[14] Et eksempel på dette er EU Data Protection Code of Conduct for Cloud Service Providers.[15]

Sådanne adfærdskodekser og certificeringer indeholder på nuværende tidspunkt ikke alle de nødvendige elementer for at sikre en tilstrækkelig beskyttelse i forbindelse med overførsler til tredjelande og kan derfor ikke anvendes som overførselsgrundlag.

Vejledninger

- Retningslinjer 04/2021 om adfærdskodekser som et redskab til overførsler
- Retningslinjer 07/2022 om certificering som et redskab til overførsler

[14] Jf. Databeskyttelsesforordningens artikel 40 og 42

[15] Home: EU Cloud CoC (eucoc.cloud)

5. Hvad skal jeg i øvrigt være særligt opmærksom på?

Dette afsnit beskriver kort, hvilke forhold du - udover at sikre dig et overførselsgrundlag - skal være særligt opmærksom på, når du overfører personoplysninger til et tredjeland.

5.1 Supplerende foranstaltninger ved overførsel til usikre tredjelande

EU-Domstolen afsagde den 16. juli 2020 dom i den såkaldte Schrems II-sag, hvor Privacy Shield-tilstrækkelighedsafgørelsen blev kendt ugyldig som overførselsgrundlag til USA, fordi amerikansk lovgivning ikke satte tilstrækkeligt klare rammer for de amerikanske myndigheders adgang til personoplysninger overført fra EU/EØS.[16]

I samme afgørelse fastslog EU-Domstolen, at Europa-Kommissionens standardbestemmelser stadig er gyldige som overførselsgrundlag, men at de ikke nødvendigvis i sig selv kan sikre et beskyttelsesniveau for personoplysninger, som i det væsentlige svarer til dét inden for EU/EØS. Disse bemærkninger fra EU-Domstolen gælder generelt for overførsler til usikre tredjelande baseret på et overførselsgrundlag i databeskyttelsesforordningens artikel 46.

Dataeksportører, som ønsker at benytte et af overførselsgrundlagene i artikel 46, er derfor forpligtede til forud for overførslen at foretage en vurdering – en såkaldt transfer impact assessment (TIA) – af forholdene i modtagerlandet med henblik på at fastslå, om det valgte overførselsgrundlag også i praksis kan sikre et tilstrækkeligt beskyttelsesniveau for de overførte oplysninger. Hvis overførselsgrundlaget ikke i sig selv kan sikre et tilstrækkeligt beskyttelsesniveau, er dataeksportøren forpligtet til at tilvejebringe såkaldte supplerende foranstaltninger.

Det Europæiske Databeskyttelsesråd har på den baggrund udarbejdet en række anbefalinger til dataeksportører.[17] Anbefalingerne er opbygget som en "køreplan" for hvilke skridt, du som dataeksportør skal foretage med henblik på at vurdere, om du skal sørge for supplerende foranstaltninger, når du overfører personoplysninger til et usikkert tredjeland. Det følger af anbefalingerne, at du som det første bør sikre dig et grundigt overblik ved at kortlægge alle dine overførsler. Dernæst skal du afklare, hvilket overførselsgrundlag, du kan benytte, herunder om dataimportøren er omfattet af en gyldig tilstrækkelighedsafgørelse.

Hvis du benytter et af de overførselsgrundlag, som er beskrevet i afsnit 4 ovenfor, skal du sikre dig, at overførselsgrundlaget også er effektivt i praksis. Dette vil ikke være tilfældet, hvis dataimportøren på grund af lovgivning og/eller praksis i tredjelandet, der finder anvendelse på den konkrete overførsel, er forhindret i at opfylde sine forpligtelser i henhold til det valgte overførselsgrundlag.

Det vil især være relevant at undersøge offentlige myndigheders praksis i et tredjeland, hvis:

1) Tredjelandets lovgivning formelt lever op til EU's standarder, men i praksis ikke efterleves af myndighederne i landet.

2) Lovgivningen i tredjelandet er mangelfuld, og praksis i tredjelandet er uforenelig med de forpligtelser, der er fastsat i det valgte overførselsgrundlag.

[16] EU-Domstolens dom af 16. juli 2020 i sagen C-311/18, Data Protection Commissioner mod Facebook Ireland Ltd og Maximillian Schrems.

[17] Henstilling nr. 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger; vedtaget den 10. november 2020

3) De overførte oplysninger eller dataimportøren er omfattet af problematisk lovgivning i tredjelandet.

Det vil i de fleste tilfælde være naturligt, hvis du som dataeksportør inddrager dataimportøren i tredjelandet i vurderingen, da denne typisk vil have et bedre lokalkendskab. Ved undersøgelsen af praksis i et tredjeland vil det også være muligt til en vis grad at lægge vægt på dataimportøren i tredjelandets praktiske erfaringer. Bilag 3 i Det Europæiske Databeskyttelsesråds anbefalinger indeholder også en (ikke-udtømmende) liste over mulige kilder, som du kan lade indgå i din vurdering.

Det kan også være, at brancheorganisationer eller lignende kan hjælpe dig i forhold til den vurdering, som du skal foretage. Endelig kan du konsultere andre informationskilder, som eksempelvis risikovurderinger fra Center for Cybersikkerhed[18].

Der er som udgangspunkt ingen metodekrav til den vurdering, som du skal foretage, men det er vigtigt, at du dokumenterer, hvilke overvejelser og beslutninger der ligger til grund for din vurdering, og at du vil kunne redegøre for disse efterfølgende.

Hvis du vurderer, at det overførselsgrundlag, du har valgt, ikke er effektivt i praksis som følge af problematisk lovgivning og/eller praksis i tredjelandet, skal du sørge for passende supplerende foranstaltninger for at imødegå dette.

I anbefalingerne fra EDPB er der angivet en række eksempler på sådanne foranstaltninger, som både kan være tekniske, organisatoriske og kontraktuelle. Der er endvidere udarbejdet en række eksempler på anvendelse af supplerende foranstaltninger i praksis, både hvor disse vil kunne anses for tilstrækkelige, og hvor det ikke vil være tilfældet. Generelt kan man sige, at tekniske foranstaltninger altid vil være nødvendige, og at organisatoriske og kontraktuelle foranstaltninger derfor typisk ikke vil kunne stå alene.

Endelig følger det af anbefalingerne, at du løbende skal vurdere, om forholdene i tredjelandet har ændret sig, og om det giver anledning til en ændring af din vurdering af, hvilke supplerende foranstaltninger der i givet fald er behov for. Du kan også her med fordel inddrage dataimportøren.

Eksempel 11

Eksempel på vurdering af forhold i et usikkert tredjeland

En konsulentvirksomhed ønsker at indgå et samarbejde med en hosting service-udbyder i et usikkert tredjeland. Samarbejdet vil indebære, at der løbende bliver overført personoplysninger til tredjelandet.

Konsulentvirksomheden vil gerne bruge Europa-Kommissionens standardbestemmelser som overførselsgrundlag og undersøger med hjælp fra hosting service-udbyderen, om der er noget i den gældende lovgivning og praksis i tredjelandet, der kan påvirke effektiviteten af overførselsgrundlaget i forhold til den specifikke overførsel.

Konsulentvirksomheden retter derudover henvendelse til sin brancheforening vedrørende eventuelle yderligere oplysninger om forholdene i tredjelandet.

På baggrund af de oplysninger, som konsulentvirksomheden modtager, vurderer konsulentvirksomheden, at der i tredjelandet er lovgivning, der giver tredjelandets myndigheder adgang til de overførte personoplysninger i et meget videre omfang, end hvad der er tilladt i EU. Det skyldes bl.a., at lovgivningen i tredjelandet giver

[18] https://cfcs.dk/da/cybertruslen/

myndighederne ubegrænset adgang til de overførte personoplysninger, og at de berørte personer ikke har nogen adgang til domstolsprøvelse i tredjelandet.

Konsulentvirksomheden har herefter to valgmuligheder:

1. Sørge for passende supplerende foranstaltninger, der sammen med overførselsgrundlaget sikrer et beskyttelsesniveau, som i det væsentlige svarer til niveauet i EU/EØS
2. Undlade at overføre personoplysninger

Vejledninger

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

5.2 Opfyldelse af oplysningspligten

Når du som dataansvarlig vil overføre personoplysninger til et tredjeland eller en international organisation, skal du oplyse den registrerede om dette. Det gælder både, når du indsamler oplysningerne direkte hos den registrerede, og når du indsamler oplysningerne hos andre.

Ud over denne generelle forpligtelse til at oplyse de registrerede om overførslen, gælder følgende særlige forpligtelser:

Hvis dataimportøren er omfattet af en tilstrækkelighedsafgørelse vedtaget af Europa-Kommissionen, skal du oplyse den registrerede om, at overførslen sker på dette grundlag.

Hvis overførslen sker på grundlag af databeskyttelsesforordningens artikel 46, skal du konkret oplyse, om du sikrer de fornødne garantier gennem Europa-Kommissionens standardbestemmelser, bindende virksomhedsregler eller et af de andre overførselsgrundlag i artikel 46. Du skal også forklare, hvordan den registrerede kan få en kopi af de fornødne garantier, og hvor de ellers kan tilgås, f.eks. på virksomhedens hjemmeside.

Hvis overførslen sker på baggrund af undtagelsen i databeskyttelsesforordningens artikel 49, stk. 1, andet afsnit, skal du oplyse om de passende garantier, du skal sikre i henhold til denne bestemmelse. Derudover skal du også underrette den registrerede om de vægtige, legitime interesser, du forfølger med overførslen.

Du kan læse mere om oplysningspligten i Datatilsynets vejledning om registreredes rettigheder.[19] Vejledningen beskriver bl.a., hvordan og hvornår du skal give oplysningerne til den registrerede.

Vejledningen indeholder også en skabelon til brug for opfyldelsen af oplysningspligten, der kan bruges til inspiration.

[19] https://www.datatilsynet.dk/Media/C/0/Registreredes%20rettigheder.pdf

Den udfyldte skabelon kunne eksempelvis se sådan ud:

"Overførsel til modtagere i tredjelande, herunder internationale organisationer.

Vi vil overføre dine personoplysninger til modtagere uden for EU og EØS. Det drejer sig om vores datterselskab, Datterselskab Ltd, som er beliggende i Singapore. Vi kan oplyse, at vi bruger Europa-Kommissionens standardbestemmelser som overførselsgrundlag for at sikre beskyttelsen af dine personoplysninger.

Du kan få udleveret en kopi af aftalen med vores datterselskab ved at kontakte vores DPO, hvis kontaktoplysninger fremgår under afsnit x"

5.3 Behandlingssikkerhed

Reglerne om behandlingssikkerhed i databeskyttelsesforordningen handler overordnet set om, at du som dataansvarlig eller databehandler skal sikre et tilstrækkeligt sikkerhedsniveau for den behandling af personoplysninger, som du foretager. Det vil i praksis sige, at du på baggrund af en vurdering af risikoen for de registreredes rettigheder, en såkaldt risikovurdering, skal træffe passede tekniske og organisatoriske foranstaltninger for at imødegå de identificerede risici.

Kravene til behandlingssikkerhed gælder også, hvis du eksempelvis overvejer at outsource din opgave med at håndtere eller opbevare personoplysninger til en virksomhed i et tredjeland. Du skal i den situation overveje, hvordan du kan opretholde det sikkerhedsniveau, som du har fastlagt, når oplysningerne bliver behandlet i tredjelandet. I den forbindelse skal du overveje, om det kræver yderligere eller andre sikkerhedsforanstaltninger, når oplysningerne skal behandles uden for EU/EØS. Der er ikke tale om, at du skal foretage en ny risikovurdering, men at du i din generelle risikovurdering tager højde for, at du ønsker at behandle oplysningerne i et tredjeland. Dette gælder også i de situationer, hvor du selv behandler oplysningerne i et tredjeland, og der dermed ikke er tale om en overførsel i databeskyttelsesforordningens forstand.

I den forbindelse skal du huske, at en dataansvarlig er ansvarlig for sine behandlingsaktiviteter, uanset hvor i verden, de finder sted. Du skal derfor være opmærksom på, om tredjelandets retlige rammer kan have en indvirkning på din evne til at overholde databeskyttelsesforordningen, f.eks. på grund af modstridende nationale love eller uforholdsmæssig myndighedsadgang i tredjelandet. Som følge af din forpligtelse til at være ansvarlig for og være i stand til at påvise overholdelse af databeskyttelsesprincipperne og til at gennemføre tekniske og organisatoriske foranstaltninger, der tager hensyn til de konkrete risici forbundet med behandlingen, kan du som dataansvarlig meget vel måtte konkludere, at det vil kræve omfattende sikkerhedsforanstaltninger — eller at det ikke vil være lovligt — at gennemføre eller fortsætte en specifik behandlingsaktivitet i et tredjeland, også selv om der ikke er tale om en overførsel i databeskyttelsesforordningens forstand.

Der er som udgangspunkt ingen krav til den metode, du anvender ved udarbejdelsen af din risikovurdering. Det er dog vigtigt, at du dokumenterer, hvilke overvejelser og beslutninger du har gjort dig, og at du vil kunne redegøre for disse efterfølgende.

Risikovurderingen benyttes til at fastlægge, hvilket niveau af behandlingssikkerhed, du skal sikre. Hvis du ønsker at behandle personoplysninger i et tredjeland, vil du konkret skulle vurdere, om der er behov for yderligere sikkerhedsforanstaltninger som følge af eksempelvis problematisk lovgivning i det pågældende tredjeland.

Selv om mange af de samme momenter skal tages i betragtning, er der ikke her tale om en vurdering, der sigter mod at fastlægge, om du lovligt kan overføre personoplysninger til et tredjeland, herunder om forholdene i tredjelandet griber forstyrrende ind i dit valgte overførselsgrundlag. Denne vurdering, som populært betegnes som en transfer impact assessment (TIA), er beskrevet ovenfor i afsnit 5.1.

Vejledninger

Du kan læse mere om kravene til behandlingssikkerhed på Datatilsynets hjemmeside: Behandlingssikkerhed og databeskyttelse gennem design og standardindstillinger (datatilsynet.dk)

Du kan læse mere om risikovurderinger på Datatilsynets hjemmeside: Risikovurdering (datatilsynet.dk)

5.4 Hvad sker der, hvis reglerne ikke overholdes?

Hvis en registreret klager over en overførsel af personoplysninger til et usikkert tredjeland, er Datatilsynet som udgangspunkt forpligtet til at undersøge, om overførslen overholder reglerne i databeskyttelsesforordningen. Datatilsynet har derudover som tilsynsmyndighed mulighed for at tage sager op på eget initiativ.

Hvis Datatilsynet finder, at der er overført personoplysninger til et tredjeland i strid med databeskyttelsesforordningens regler, kan tilsynet bl.a. udtale kritik eller give påbud om at suspendere overførslen af oplysninger. Afhængigt af omstændighederne i den enkelte sag kan en politianmeldelse også komme på tale.

5.5 Anmodninger fra myndigheder i tredjelande

Hvis du som dataansvarlig eller databehandler modtager en anmodning fra en myndighed i et tredjeland om at overføre personoplysninger, baseret på en dom eller afgørelse fra den pågældende myndighed, skal du være opmærksom på følgende:

Domme eller afgørelser fra tredjelandes myndigheder kan kun anerkendes og håndhæves i EU/EØS, hvis dette følger af en international aftale mellem tredjelandet og EU/EØS eller en medlemsstat.[20] Virksomheder i EU/EØS kan i nogle tilfælde være underlagt et tredjelands lovgivning, eksempelvis fordi de er datterselskaber af virksomheder i tredjelandet eller på anden måde har tilknytning til landet. At virksomheden efter et tredjelands lovgivning er forpligtet til at udlevere bestemte oplysninger betyder dog ikke, at det vil være i overensstemmelse med databeskyttelsesreglerne at overføre oplysningerne.

Hvis du imødekommer en anmodning fra en myndighed i et tredjeland om at overføre personoplysninger, vil dette være en overførsel omfattet af databeskyttelsesforordningens regler. Der skal derfor findes hjemmel til behandlingen i forordningens artikel 6 og et overførselsgrundlag eller en relevant undtagelse i forordningens kapitel V, før du lovligt kan overføre oplysningerne.

Anmodningen udgør ikke et overførselsgrundlag.

[20] jf. databeskyttelsesforordningens artikel 48

6. Er der tale om en særlig situation?

I dette afsnit kan du læse om en række særlige situationer, hvor det er muligt at overføre personoplysninger til et usikkert tredjeland uden et overførselsgrundlag.

Du kan som dataeksportør i nogle særlige situationer overføre personoplysninger til et tredjeland, selvom Europa-Kommissionen ikke har truffet afgørelse om et tilstrækkeligt beskyttelsesniveau i tredjelandet, og selvom du ikke har et overførselsgrundlag under artikel 46.

Det gælder, hvis en af de særlige undtagelser i artikel 49 i databeskyttelsesforordningen finder anvendelse.

Fordi der er tale om undtagelser, kan du kun anvende dem i meget begrænset omfang, og undtagelserne skal fortolkes restriktivt, således at undtagelsen ikke bliver reglen. De kan derfor generelt ikke bruges i forhold til overførsler, der må betegnes som masseoverførsler eller systematiske overførsler, da dette vil være i strid med undtagelsens karakter.

De følgende afsnit beskriver kort de særlige situationer, hvor du kan overføre personoplysninger til et tredjeland. Du kan læse mere om de særlige situationer i Det Europæiske Databeskyttelsesråds vejledning herom, som også indeholder en detaljeret gennemgang af betingelserne for at anvende de forskellige undtagelser.[21]

Vejledninger

Retningslinjer 2/2018 vedrørende undtagelser i artikel 49 i forordning 2016/679

6.1 Den registrerede har givet udtrykkeligt samtykke til overførslen

Du kan i nogle tilfælde overføre personoplysninger til et tredjeland, hvis den registrerede person har givet sit *udtrykkelige samtykke* til overførslen.

Du skal sikre dig, at samtykket fra den registrerede er gyldigt. Det betyder, at du skal have samtykke i form af en frivillig, specifik, informeret og utvetydig viljestilkendegivelse fra den registrerede. Du skal dertil være opmærksom på, at der er særligt strenge betingelser til et gyldigt samtykke, når det skal anvendes til brug for overførsler.

Herudover skal du sørge for at informere den registrerede om de mulige risici, som overførslen kan medføre for den registrerede. Du skal give den registrerede informationen, før vedkommende giver samtykke til overførslen af sine personoplysninger.

Du skal desuden være opmærksom på, at offentlige myndigheder ikke kan benytte samtykke, når de handler som led i deres offentligretlige beføjelser.

[21] Retningslinjer 2/2018 vedrørende undtagelser i artikel 49 i forordning 2016/679; vedtaget den 25. maj 2018

Eksempel 12

Fodboldstævne i Sydafrika

En sportsklub har et oldboys-hold, som ønsker at deltage i et stævne i Sydafrika. Der er tale om frivillige medlemmer, som ikke er ansat i klubben.

I forbindelse med at klubben skal arrangere holdets deltagelse i stævnet, skal klubben oplyse stævnearrangøren i Sydafrika om medlemmernes navne. Klubben skal derudover også booke hotel til spillerne i Sydafrika. I den forbindelse skal klubben oplyse hotellet om spillernes navne og kontaktoplysninger.

Sportsklubben informerer forud for overførsel af oplysningerne spillerne på old boys-holdet om de mulige risici forbundet med at overføre ovennævnte personoplysninger til Sydafrika. Herefter sikrer sportsklubben, at alle spillerne på old boys-holdet udtrykkeligt har givet samtykke til den specifikke overførsel.

På den baggrund kan sportsklubben overføre de relevante oplysninger om spillerne til henholdsvis stævnearrangøren og hotellet.

Vejledninger

- Datatilsynets vejledning om samtykke
- Retningslinjer 5/2020 vedrørende samtykke i henhold til forordning 2016/679

6.2 Overførslen er nødvendig af hensyn til indgåelse eller opfyldelse af en kontrakt mellem dig og den registrerede

Du kan overføre personoplysninger til et tredjeland, hvis det er nødvendigt for dig som dataeksportør af hensyn til opfyldelse af en kontrakt mellem den registrerede og dig. Det samme gælder, hvis overførslen er nødvendig af hensyn til gennemførsel af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelsen af kontrakten.

Du kan kun anvende denne undtagelse, hvis overførslen er nødvendig. Det betyder, at der skal være en tæt og betydelig forbindelse mellem overførslen af personoplysninger og kontraktens formål. Dertil kommer, at overførslen kun må være lejlighedsvis.

Du skal være opmærksom på, at offentlige myndigheder ikke kan benytte denne undtagelse, når de handler som led i deres offentligretlige beføjelser.

Eksempel 13

Rejsebestilling

Et dansk rejsebureau har indgået en aftale med en gruppe rejsende om at arrangere en rygsækrundrejse i Peru. I den forbindelse sender rejsebureauet de rejsendes navne til en lokal buschauffør i Lima, som skal køre de rejsende fra Lima til Machu Picchu.

Hvis det er en del af aftalen mellem rejsebureauet og gruppen af rejsende, at bureauet skal sørge for, at de rejsende bliver fragtet med bus fra Lima til Machu Picchu, da vil rejsebureauet kunne sende de rejsendes navne til den lokale buschauffør i Lima, hvis navnene er en forudsætning for, at chaufføren kan køre de rejsende til Machu Picchu.

Hvis samarbejdet mellem rejsebureauet og buschaufføren får karakter af et mere permanent samarbejde, vil der være behov for at etablere et overførselsgrundlag som beskrevet i afsnit 4.

6.3 Overførslen er nødvendig af hensyn til indgåelse eller opfyldelse af en kontrakt mellem dig og en anden end den registrerede

Du kan overføre personoplysninger til et tredjeland, hvis overførslen er nødvendig af hensyn til indgåelsen eller opfyldelsen af en kontrakt med en anden fysisk eller juridisk person end den registrerede. Det er dog et krav, at indgåelsen eller opfyldelsen af kontrakten er i den registreredes interesse. Det vil sige, at det ikke er en betingelse, at kontrakten er indgået med den registrerede som part.

Du kan kun anvende undtagelsen, når overførslen er nødvendig. Det betyder, at der skal være en tæt og betydelig forbindelse mellem overførslen af personoplysninger og kontraktens formål. Dertil kommer, at overførslen kun må være lejlighedsvis.

Du skal være opmærksom på, at offentlige myndigheder ikke kan benytte denne undtagelse, når de handler som led i deres offentligretlige beføjelser.

Eksempel 14

Udlicitering af lønadministration

En organisation i Danmark har i forretningsøjemed udliciteret aktiviteter såsom lønforvaltning til en virksomhed i Indien. Selvom formålet med overførslen af oplysninger er forvaltning af arbejdstagerens løn, vil organisationen ikke kunne bruge undtagelsesbestemmelsen nævnt i dette afsnit. Det skyldes, at det ikke kan fastslås, at der er en tæt og betydelig forbindelse mellem overførslen og en kontrakt indgået i den registreredes (lønmodtagerens) interesse.

Eksempel 15

Bolig under udstationering

En medarbejder skal som en del af sit ansættelsesforhold hos et dansk entreprenørfirma udstationeres til Taiwan i et år. Entreprenørfirmaet skal sørge for en bolig til medarbejderen under udstationeringen. I den forbindelse indgår entreprenørvirksomheden en kontrakt om leje af bolig med et boligudlejningsselskab i Taiwan. Som led i indgåelsen af kontrakten sender entreprenørvirksomheden oplysninger om den pågældende medarbejders navn og kontaktoplysninger til boligudlejningsselskabet i Taiwan.

Kontrakten er indgået med henblik på at sikre medarbejderen en bolig under sit ophold i Taiwan. Derudover er overførslen af personoplysninger om medarbejderen en forudsætning for udlejning af boligen til den pågældende, hvorfor det må lægges til grund, at der er en tæt og betydelig forbindelse mellem overførslen og kontrakten. Det vil derfor i dette tilfælde være muligt for entreprenørvirksomheden at overføre de pågældende oplysninger.

6.4 Overførslen er nødvendig af hensyn til vigtige samfundsinteresser

Du kan overføre personoplysninger til et tredjeland, hvis det er nødvendigt af hensyn til vigtige samfundsinteresser. Det er kun vigtige samfundsinteresser, som er anerkendt i EU-retten eller retten i den medlemsstat, som du som dataeksportør er underlagt, der kan danne grundlag for anvendelse af denne undtagelse.

Som eksempler på vigtige samfundsinteresser kan nævnes international udveksling af oplysninger mellem konkurrencemyndigheder eller udveksling af personoplysninger af hensyn til folkesundheden, herunder i tilfælde af kontaktsporing i forbindelse med smitsomme sygdomme.

Eksempel 16

Udveksling af sundhedsoplysninger

En dansk statsborger bliver efter en ferie i Burkina Faso indlagt med symptomer på ebola virus. Da den pågældende borger har rejst med en gruppe russiske statsborgere, vælger de danske sundhedsmyndigheder at tage kontakt til de russiske sundhedsmyndigheder for at orientere dem om det mulige tilfælde af ebola. I den forbindelse overføres der oplysninger om den danske statsborger til Rusland.

Da det er en vigtig samfundsinteresse - i såvel Danmark som i Rusland - at begrænse antallet af smittede med en potentiel meget dødelig sydom som ebola, og overførslen i denne situation må siges at være nødvendig af hensyn til opfyldelsen af denne vigtige samfundsinteresse, vil de danske sundhedsmyndigheder kunne overføre oplysningerne til Rusland.

6.5 Overførslen er nødvendig, for at et retskrav kan fastlægges, gøres gældende eller forsvares

Du kan overføre personoplysninger til et tredjeland, hvis det er nødvendigt for, at et retskrav kan fastlægges, gøres gældende eller forsvares.

Retskrav henviser til domme og afgørelser truffet af administrative myndigheder, som er anerkendt i EU/EØS.

Det er et krav, at overførslen af personoplysninger skal være *nødvendig* for, at det pågældende retskrav kan fastlægges, gøres gældende eller forsvares. Det betyder, at du skal sikre dig, at der er en tæt og betydelig forbindelse mellem nødvendigheden af at overføre de pågældende personoplysninger og fastlæggelsen, fremførelsen eller forsvaret af det specifikke retskrav. Dertil kommer, at overførslen kun må være lejlighedsvis.

Eksempel 17

Overførsel af personoplysninger til brug for retssag

Myndighederne i Thailand rejser tiltale for kartelvirksomhed mod et flyselskab, der er hjemmehørende i Frankrig. Til brug for sit forsvar i retssagen, der skal foregå i Thailand, har flyselskabet behov for at overføre personoplysninger til flyselskabets thailandske advokat. Da oplysningerne er nødvendige for, at virksomheden i Frankrig kan forsvare sig i retssagen, kan virksomheden overføre personoplysningerne til Thailand.

6.6 Overførslen er nødvendig for at beskytte vitale interesser

Du kan overføre personoplysninger til et tredjeland, hvis overførslen er nødvendig for at beskytte den registrerede eller andre personers vitale interesser.

Du kan f.eks. gøre brug af undtagelsen i tilfælde af akut behov for lægebehandling, hvor en overførsel af personoplysninger derfor er direkte *nødvendig* for at give den påkrævede lægebehandling. I sådanne tilfælde er det lagt til grund i databeskyttelsesforordningen, at den overhængende risiko for alvorlig skade på den registrerede vejer tungere end databeskyttelseshensyn. Du skal være opmærksom på, at du ikke kan bruge undtagelsen til overførsel af helbredsoplysninger til tredjelande, hvis formålet med overførslen ikke er at behandle den registrerede eller en anden person. Du kan derfor f.eks. ikke bruge undtagelsen til at overføre personoplysninger til et tredjeland for at udføre almen medicinsk forskning.

Du kan heller ikke bruge undtagelsen, når den registrerede er i stand til at træffe en beslutning, og der kan anmodes om vedkommendes samtykke.

Eksempel 18

Overførsel af sundhedsjournal

En dansk kvinde bliver under en ferie i Brasilien fundet bevidstløs på gaden og bliver i den forbindelse indlagt på et lokalt sygehus. Under indlæggelsen har det brasilianske sygehus - til brug for behandlingen - behov for nogle specifikke sundhedsoplysninger fra Danmark.

Det er i den indlagte kvindes vitale interesse, at hun modtager en så god og korrekt behandling som muligt, og det må antages at overførslen vil være direkte nødvendig for at give den påkrævede behandling. Det må ligeledes lægges til grund, at det - grundet kvindens tilstand - vil være praktisk umuligt at indhente et samtykke. Der kan således overføres oplysninger fra de danske sundhedsmyndigheder til det brasilianske sygehus.

6.7 Overførsel fra et register

Du kan overføre personoplysninger til et tredjeland, hvis oplysningerne kommer fra et register, der ifølge EU-ret eller EU/EØS-landenes lovgivning er beregnet til at informere offentligheden. Registeret skal være tilgængeligt for offentligheden generelt eller for personer, der kan bevise, at de har en legitim interesse heri.

Private registre er ikke omfattet af denne undtagelse.

Du må ikke på baggrund af undtagelsen overføre alle personoplysninger eller hele kategorier af personoplysninger i et register. F.eks. vil det ikke være lovligt at overføre alle helbredsoplysninger for personer af en bestemt religiøs overbevisning i et offentligt register.

6.8 Overførslen er nødvendig af hensyn til dine vægtige legitime interesser

Som en sidste udvej kan du på en række specifikke, udtrykkeligt angivne betingelser[22] overføre personoplysninger til et tredjeland, hvis overførslen er nødvendig af hensyn til vægtige legitime interesser, som du som dataansvarlig forfølger. Dette er kun muligt, hvis den registreredes interesser eller rettigheder ikke går forud for dine vægtige legitime interesser. Det er et krav, at du i forbindelse med afvejningen foretager en vurdering af alle omstændigheder omkring overførslen og på den baggrund sikrer passende garantier for beskyttelsen af de overførte personoplysninger.

Du skal være opmærksom på, at du kun kan bruge undtagelsen i enkeltstående tilfælde. Derudover skal du kunne påvise, at det ikke var muligt at anvende et overførselsgrundlag i artikel 45 eller 46 eller én af de andre undtagelser i artikel 49.

Ud over de nævnte betingelser er det et krav, at du underretter Datatilsynet om overførslen, og at du underretter den registrerede om de vægtige interesser, som begrunder overførslen. Se tillige om de særlige krav til opfyldelse af oplysningspligten i afsnit 5.2 ovenfor.

Det er væsentligt at understrege, at det kun er muligt at benytte undtagelsen i meget begrænset omfang. Du skal også være opmærksom på, at offentlige myndigheder ikke kan benytte denne undtagelse, når de handler som led i deres offentligretlige beføjelser.

[22] Se Artikel 49, stk. 1, andet afsnit, og betragtning 113 til Databeskyttelsesforordningen

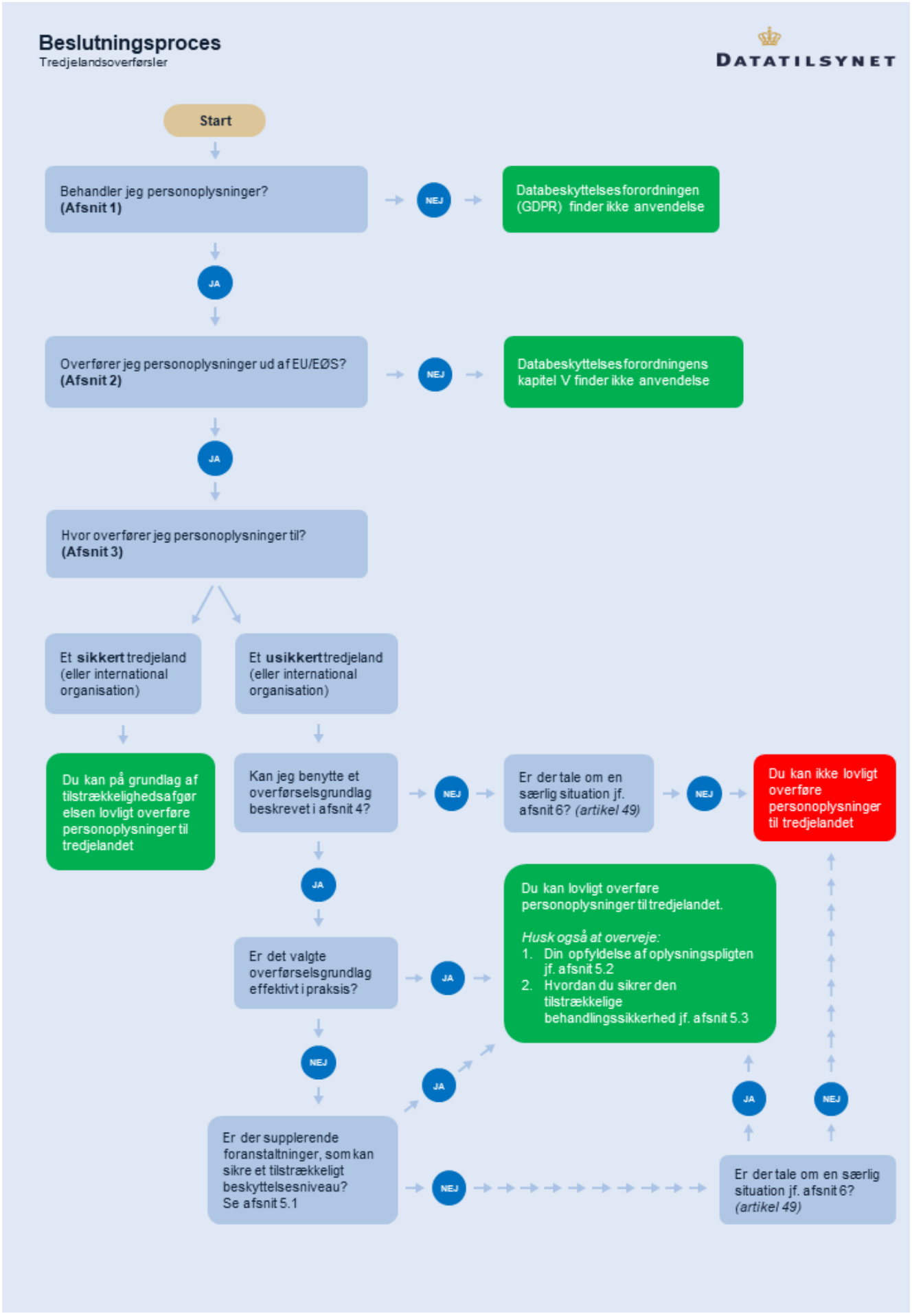
Bilag

Her finder du et skema med overførselsgrundlagene i artikel 46 og et flowchart, der illustrerer beslutningsprocessen ved en tredjelandsoverførsel.

Bilag 1: Skema med overførselsgrundlagene i artikel 46

Overførselsgrundlag	Målgruppe	Ulemper	Fordele
Standardbestemmelser *Art. 46, stk. 2, litra c) og d)*	• Offentlige myndigheder og private virksomheder	• Begrænset mulighed for at foretage ændringer	• Intet krav om godkendelse fra Datatilsynet • Kan anvendes i de fleste overførselssituationer • Moduler kan kombineres, så én aftale kan dække flere overførselssituationer • Der kan løbende tilføjes/fjernes parter • Kan indgå i databehandleraftalen eller hovedaftalen, så man kan nøjes med ét samlet aftaledokument
Ad hoc-kontrakter *Art. 46, stk. 3, litra a)*	• Offentlige myndigheder og private virksomheder	• Skal godkendes af Datatilsynet og EDPB • Kan være ressourcekrævende at udarbejde	• Anvendes typisk som alternativ til standardbestemmelserne • Du har selv indflydelse på indhold og udformning og kan skræddersy kontrakten til den specifikke overførselssituation
Bindende virksomhedsregler *Art. 47, jf. art. 46, stk. 2, litra b)*	• Større koncerner og grupper af foretagender, der udøver en fælles økonomisk aktivitet	• Skal godkendes af Datatilsynet og EDPB • Kan være ressourcekrævende at udarbejde • Kan kun anvendes internt i koncernen	• Kan dække alle overførsler indenfor en koncern • Kan indgå som en del af koncernens samlede compliance-opsætning
Retligt bindende instrument *Art. 46, stk. 2, litra a)*	• Offentlige myndigheder • Private virksomheder, hvis dette fremgår af det retligt bindende instrument	• Kan være ressourcekrævende at udarbejde	• Intet krav om godkendelse fra Datatilsynet • Kan dække alle overførsler omfattet af det retligt bindende instrument
Administrative ordninger *Art. 46, stk. 3, litra b)*	• Offentlige myndigheder	• Skal godkendes af Datatilsynet og EDPB	• Kan dække alle overførsler mellem de involverede myndigheder
Adfærdskodekser *Art. 46, stk. 2, litra e)*	• Offentlige myndigheder og private virksomheder	• Endnu ingen godkendte adfærdskodekser til brug for overførsler	• Kan dække alle overførsler til en dataimportør, som har tilsluttet sig et godkendt adfærdskodeks
Certificeringsordninger *Art. 46, stk. 2, litra f)*	• Offentlige myndigheder og private virksomheder	• Endnu ingen godkendte certificeringsordninger til brug for overførsler	• Kan dække alle overførsler til en certificeret dataimportør

Bilag 2: Flowchart: Beslutningsprocessen ved en tredjelandsoverførsel



Vejledning om overførsel til tredjelande

Udgivet af:
Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 33 19 32 00
dt@datatilsynet.dk
datatilsynet.dk

Foto: Tredjelandsoverførsler

ISBN (www): Klik og skriv ISBN-nummber

Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 33 19 32 00
dt@datatilsynet.dk
datatilsynet.dk