Vejledning

Overførsel af personoplysninger til tredjelande

Juli 2021 (3. udgave)

DATATILSYNET

Indhold

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 også læse mere om tredjelandsoverførsler på Datatilsynets hjemmeside:
www.datatilsynet.dk/internationalt/tredjelandsoverfoersler

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 1 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?
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 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 efter 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 en 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 sagt med andre ord undersøge, om du overfører personoplysninger ud af EU/EØS, og hvor du i så fald overfører personoplysningerne til.

2.1 Hvad er en overførsel?

Den dataansvarlige eller databehandleren, som overfører personoplysninger ud af EU/EØS bliver typisk betegnet *”dataeksportøren”,* og den dataansvarlige eller databehandleren i tredjelandet, som personoplysningerne bliver overført til, bliver typisk betegnet *”dataimportøren”*.[2]

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.

Der vil som udgangspunkt være tale om en overførsel til et tredjeland, når de personoplysninger, du som dataansvarlig eller databehandler behandler, forlader EU/EØS eller gøres tilgængelige uden for EU/EØS. Det gælder, uanset om overførslen af personoplysninger sker til en virksomhed eller en myndighed.

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

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 fysisk forlader EU/EØS .

[2] Hvis en databehandler på vegne af en dataansvarlig i EU/EØS overfører personoplysninger til et tredjeland, er det den dataansvarlige, der anses som ”dataeksportøren”. Hvis databehandleren overfører personoplysninger til et tredjeland på vegne af en dataansvarlig uden for EU/EØS, som ikke er omfattet af databeskyttelsesforordningens anvendelsesområde, vil det derimod være databehandleren, der anses for ”dataeksportør”.

Eksempel 2

Outsourcing af IT-support

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

Der er imidlertid tale om en overførsel til et tredjeland, da det er muligt for den indiske virksomhed (dataimportøren) at tilgå oplysningerne uden for EU/EØS. Det gør ingen forskel, at den indiske virksomheds medarbejdere eksempelvis ikke forstår dansk, eller at de instrueres i ikke at søge i personoplysningerne.

Der lægges i eksemplet vægt på, at oplysningerne gøres tilgængelige for personer, der befinder sig i et tredjeland, og at databehandleren typisk fortsat vil foretage en behandling af oplysningerne på baggrund af en instruks fra den dataansvarlige, uanset at databehandleren ikke har adgang til at printe eller lagre oplysningerne.

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. Konsulentvirksomheden er således databehandler for den kinesiske virksomhed.

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 overføres tilbage til virksomheden i Kina, vil dette imidlertid være en overførsel, fordi personoplysningerne fysisk forlader EU/EØS. 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, hvilket udføres fra Ukraine, hvor cloud-udbyderen er etableret.

Hvis cloud-udbyderen får adgang til personoplysninger, når denne foretager vedligeholdelse og fejlretning, vil der i disse tilfælde være tale om en overførsel af personoplysninger til Ukraine, hvor cloud-udbyderen befinder sig.

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 nyhedsbreve, til virksomheden i Chile.

Når modevirksomheden sender e-mailadresser på sine kunder til virksomheden i Chile, er der tale om en overførsel af personoplysninger til et tredjeland, idet oplysningerne geografisk forlader EU/EØS.

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 bl.a. inkludere 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, sker der således en overførsel af deres personoplysninger, idet oplysningerne geografisk forlader EU/EØS og lagres 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 geografisk forlader EU/EØS. Selvom de to virksomheder tilhører samme koncern, er de hver især dataansvarlige for behandlingen 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 virksomhedens netværk og tilgår e-mails mv., som indeholder personoplysninger, vil der ikke være tale om en overførsel til et tredjeland, fordi medarbejderne ikke anses for at være adskilt fra IT-leverandøren (den dataansvarlige). Behandlingen foretages således af den samme dataansvarlige, idet medarbejderne ikke anses for selvstændige dataansvarlige eller databehandlere for IT-leverandøren. Hvis medarbejderne derimod overlader personoplysningerne til den pakistanske virksomhed, vil der være tale om en overførsel til et tredjeland.

Selvom databeskyttelsesforordningens regler om overførsel til tredjelande således ikke finder anvendelse i eksemplet, skal IT-leverandøren stadigvæk sikre overholdelse af databeskyttelsesforordningens øvrige regler, når medarbejderne behandler personoplysninger under forretningsrejsen. Det betyder i praksis, at medarbejderne ikke kan behandle personoplysninger under deres forretningsrejse, hvis IT-leverandøren ikke kan 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 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.

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 fra den danske virksomhed.

Selvom databeskyttelsesforordningens regler om overførsel til tredjelande således ikke finder anvendelse, 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 kan 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 et 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 sikre tilstrækkelige 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 anses for selvstændig dataansvarlig for den pågældende behandling.

3. Hvor overfører jeg personoplysninger til?

I dette afsnit kan du læse om, hvornår du skal sikre dig et såkaldt overførselsgrundlag, når du overfører personoplysninger til tredjelande mv.

I de følgende afsnit beskrives det nærmere, hvordan du skal forholde dig, hvis du overfører personoplysninger til de forskellige typer af tredjelande mv.

3.1 EU- og EØS-lande

Hvis den behandling af personoplysninger, som du foretager, indebærer, at personoplysninger bliver overført til eller fra et andet EU-land eller et EØS-land (Island, Lichtenstein og Norge), finder reglerne i databeskyttelsesforordningen om overførsel ikke anvendelse.

Særligt om Storbritannien og Brexit

Som følge af Brexit har Storbritannien med virkning fra den 1. januar 2021 været at betragte som et tredjeland i databeskyttelsesforordningens forstand.

I forbindelse med Brexit indgik EU og Storbritannien en aftale om, at overførsler fra EU/EØS til Storbritannien kunne fortsætte uændret indtil udgangen af juni 2021.

Europa-Kommissionen har efterfølgende den 28. juni 2021 vedtaget en tilstrækkelighedsafgørelse for Storbritannien, hvilket betyder, at Storbritannien skal betragtes som et sikkert tredjeland. Det indebærer, at der ikke er behov for at tilvejebringe et såkaldt overførselsgrundlag, når man overfører personoplysninger til Storbritannien.

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 i det væsentlige svarer til beskyttelsesniveauet i EU/EØS. I daglig tale kaldes lande, som er omfattet af en tilstrækkelighedsafgørelse, for ”sikre tredjelande”.

Ved sin vurdering foretager Europa-Kommissionen bl.a. en analyse af de regler, der gælder for behandling af personoplysninger i tredjelandet, men også en analyse af, hvordan tredjelandet efterlever grundlæggende retsstatsprincipper, giver ret til klageadgang og domstolsprøvelse mv.

Tilstrækkelighedsafgørelsen indebærer, at du kan overføre personoplysninger til det pågældende tredjeland uden at skulle tilvejebringe et såkaldt overførselsgrundlag. Hvis du ønsker at overføre personoplysninger til et tredjeland, bør du derfor som det første skridt undersøge, om Europa-Kommissionen har truffet en tilstrækkelighedsafgørelse.

Selvom der refereres til et sikkert tredjeland, skal du være opmærksom på, at Europa-Kommissionens tilstrækkelighedsafgørelse ikke altid dækker hele det pågældende land. Tilstrækkelighedsafgørelsen kan eksempelvis være begrænset til at vedrøre et bestemt område i landet, en sektor eller overførsel af en bestemt type personoplysninger.

Europa-Kommissionen foretager regelmæssige gennemgange af tilstrækkelighedsafgørelserne og kan i den forbindelse finde behov for at ændre, ophæve eller erstatte tilstrækkelighedsafgørelser, f.eks. hvis forholdene i det pågældende tredjeland ændrer sig. Det kan betyde, at tredjelande, som Europa-Kommissionen tidligere har vurderet som sikre, ikke kan opretholde denne status. Du bør derfor altid orientere dig på Europa-Kommissionens hjemmeside for at få en opdateret status.

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.[3]

Figur 1

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

Figur 2

OVERSIGT OVER SIKRE OMRÅDER/SEKTORER I TREDJELANDE	
Australien	Overførsel af oplysninger om flypassagerer.
Canada	Modtagere underlagt den canadiske Personal Information Protection and Electronic Documents Act (PIPED Act).
Færøerne	Gælder kun modtagere, der er omfattet af den færøske lov om behandling af personoplysninger. Overførsler til rigsmyndighederne, dvs. eksempelvis Rigsombudsmanden, Retten på Færøerne, Politimesteren på Færøerne, Kriminalforsorgen på Færøerne mv., er ikke omfattet.
Japan	Overførsel af oplysninger til organisationer, der falder ind under den japanske Act on the Protection of Personal Information (APPI). Bemærk desuden de undtagne sektorer, herunder eksempelvis pressen, universiteter mv.

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

I nedenstående skema kan du se en oversigt over, hvilke lande Europa-Kommissionen har igangsat arbejdet med en tilstrækkelighedsafgørelse for:

Figur 3

TILSTRÆKKELIGHEDSAFGØRELSER PÅ VEJ	
Sydkorea	Den 30. marts 2021 afsluttede Europa-Kommissionen drøftelserne med Sydkorea for herefter at igangsætte den formelle beslutningsprocedure for vedtagelse af en tilstrækkelighedsafgørelse for Sydkorea.
USA	Europa-Kommissionen og de amerikanske myndigheder er i dialog om at finde en erstatning for den tidligere gældende Privacy Shield-ordning, som i visse situationer gjorde det muligt at overføre personoplysninger til USA uden et overførselsgrundlag.

3.3 Usikre tredjelande

Et tredjeland betegnes som "usikkert", hvis Europa-Kommissionen ikke har truffet en tilstrækkelighedsafgørelse som omtalt i afsnit 3.2 ovenfor. Hvis du ønsker at overføre personoplysninger til et usikkert tredjeland, skal du derfor sørge for at have et såkaldt overførselsgrundlag, som er nærmere beskrevet i afsnit 4.

Særligt om Rigsfællesskabet - Færøerne og Grønland

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

Europa-Kommissionen har truffet en tilstrækkelighedsafgørelse vedrørende Færøerne, som derfor er et sikkert tredjeland. Du skal dog i den forbindelse være opmærksom på, at rigsmyndighederne (f.eks. politiet, kriminalforsorgen og rigsombudsmanden) ikke er omfattet af tilstrækkelighedsafgørelsen, og at du derfor skal have et overførselsgrundlag for at kunne overføre personoplysninger til disse myndigheder.

Europa-Kommissionen har ikke truffet en tilstrækkelighedsafgørelse vedrørende Grønland, som derfor er et usikkert tredjeland. Det betyder, at hvis du ønsker at overføre personoplysninger til Grønland, skal du ligesom ved andre usikre tredjelande sørge for at have et overførselsgrundlag.

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 overførselsrundlag, når du overfører personoplysninger til en sådan organisation.[4] En international organisation kan f.eks. være FN og OECD.

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

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 hertil på baggrund af tilstrækkelighedsafgørelsen.

Europa-Kommissionen har på nuværende tidspunkt ikke truffet tilstrækkelighedsafgørelser i relation til internationale organisationer, men du kan holde dig opdateret herom på Europa-Kommissionens hjemmeside[5].

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

4. Hvilke overførelsesgrundlag kan jeg bruge?

I dette afsnit kan du læse om de forskellige overførselsgrundlag, som du kan vælge mellem, når du vil overføre personoplysninger til et usikkert tredjeland.

Hvis du overfører personoplysninger til et tredjeland, som Europa-Kommissionen ikke har vurderet har 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 sørger for, at du har et af de såkaldte "overførselsgrundlag", som er nævnt i databeskyttelsesforordningens artikel 46.

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, din virksomhedsstruktur, hvor hurtigt du skal bruge overførselsgrundlaget mv.

I afsnit 4.1 - 4.6 kan du læse mere om de enkelte overførselsgrundlag, og i skemaet nedenfor finder du et overblik over de forskellige overførselsgrundlag med angivelse af målgruppe samt fordele og ulemper. **(Skemaet findes også i bilag 2 i et stort format)**

Figur 4

Overførselsgrundlag	Målgruppe	Ulemper	Fordele
Standardbestemmelser	Både offentlige myndigheder og private virksomheder	• Begrænset mulighed for at foretage ændringer.	• Intet krav om godkendelse fra Datatilsynet. • Kan anvendes i de fleste overførselssituationer, og de enkelte moduler kan kombineres, så aftalen dækker flere overførselssituationer. • Der kan løbende tilføjes/fjernes parter. • Må gerne indarbejdes i databehandleraftale/hovedaftalen, så man kan nøjes med ét samlet aftaledokument.
Ad hoc kontrakt	Både 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, hvilket især er relevant, hvor man ønsker at fravige standardbestemmelserne.
Bindende virksomhedsregler	Større koncerner mv.	• Skal godkendes af Datatilsynet og EDPB. • Kan være ressourcekrævende at udarbejde. • Kan kun anvendes internt i koncernen.	• Kan dække alle overførsler internt i en koncern. • Kan indgå som del af koncernens samlede compliance set-up.
Retlig bindende instrument	Offentlige myndigheder	• Kan være ressourcekrævende at udarbejde.	• Intet krav om godkendelse fra Datatilsynet. • Kan dække alle overførsler mellem de involverede myndigheder.
Administrative ordninger	Offentlige myndigheder	• Skal godkendes af Datatilsynet og EDPB.	• Kan dække alle overførsler mellem de involverede myndigheder.

4.1 Standardbestemmelser om databeskyttelse

Et af de måske mest brugte overførselsgrundlag er Europa-Kommissionens standardbestemmelser om databeskyttelse - også kaldet standardkontrakter - 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 standardbestemmelser, 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, jf. afsnit 4.3 nedenfor.

Europa-Kommissionen har den 4. juni 2021 vedtaget nye standardbestemmelser til brug for overførsel til tredjelande. De nye standardbestemmelser består af flere særskilte moduler, som skal kombineres alt efter, hvilken overførselssituation man befinder sig i. Det har siden den 27. juni 2021 været 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 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 med brugen af standardbestemmelserne.

De nye standardbestemmelser indeholder en såkaldt ”docking clause”, hvilket gør det muligt løbende at udskifte eller tilføje parter til aftalen, hvilket særligt kan være relevant for 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.

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 aftale, som kræver godkendelse fra Datatilsynet. Se mere herom i afsnit 4.2 nedenfor.

Overgangsregler

Europa-Kommissionens tidligere standardbestemmelser til brug for overførsel fra dataansvarlig til dataansvarlig og fra dataansvarlig til databehandler er ophævet med virkning fra den 27. september 2021.

Aftaler om overførsel af personoplysninger ved brug af de tidligere standardbestemmelser, som er indgået inden den 27. september 2021, vil dog fortsat kunne anvendes

frem til den 27. december 2022. Det forudsætter dog, at den behandling, der er genstand for aftalen, forbliver uændret, og at anvendelsen af de gamle standardbestemmelser sikrer, at overførslen af personoplysninger er omfattet af de fornødne garantier.

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 kan derfor være, at du får mulighed for selv at tilpasse indholdet af kontrakten til den konkrete situation. Det kan også 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 omvendt, at de skal godkendes af Datatilsynet, der er forpligtet til at indhente en udtalelse fra Det Europæiske Databeskyttelsesråd, og den procedure tager tid. Datatilsynet anbefaler derfor typisk, at man så vidt muligt i stedet 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 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 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 gruppemedlemmerne.

Figur 5

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

Du skal være opmærksom på, at bindende virksomhedsregler skal godkendes af Datatilsynet, og at der er en særlig godkendelsesprocedure, der typisk tager 1-2 år, da andre europæiske datatilsynsmyndigheder - og i sidste ende Det Europæiske Databeskyttelsesråd - også skal inddrages i godkendelsesproceduren.

Du kan læse mere på Datatilsynets hjemmeside om, hvordan du ansøger, og hvilke krav de bindende virksomhedsregler skal opfylde. Du kan også læse nærmere om processen, herunder det forventede tidsforløb for godkendelse af dine bindende virksomhedsregler.

Vejledninger

- WP 256 - Arbejdsdokument om tjekliste over de elementer og principper, som skal være indeholdt i bindende virksomhedsregler for dataansvarlige
- WP 257 – Arbejdsdokument om tjekliste over de elementer og principper, som skal være indeholdt i bindende virksomhedsregler for databehandlere
- WP 264 – Anbefaling om standardansøgning til brug for godkendelse af bindende virksomhedsregler for dataansvarlige
- WP 265 - Anbefaling om standardansøgning til brug for godkendelse af bindende virksomhedsregler for databehandlere

Du kan finde vejledningerne på Datatilsynets hjemmeside på undersiden "Tredjelandsoverførsler" under punktet om Bindende virksomhedsregler (BCR).[6]

4.4 Adfærdskodekser og certificeringsmekanismer

Der er endnu ikke godkendt adfærdskodekser eller certificeringsmekanismer til brug for overførsel til tredjelande fra Danmark.

Adfærdskodekser og certificeringsmekanismer kan dog på sigt være interessante at benytte for små eller mellemstore virksomheder. Det skyldes bl.a., at det ikke nødvendigvis er dig som dataeksportør, som skal udarbejde adfærdskodekset eller certificeringsmekanismen. Det kan eksempelvis være brancheorganisationer mv., som udarbejder adfærdskodekser eller certificeringsmekanismer for at lette deres medlemmers overholdelse af databeskyttelsesforordningens regler.

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

[6] https://www.datatilsynet.dk/internationalt/tredjelandsoverfoersler

Du skal være opmærksom på, at der også findes adfærdskodekser og certificeringsordninger, som ikke er vedtaget med henblik på at kunne udgøre et overførselsgrundlag, og derfor ikke indeholder de nødvendige elementer i denne henseende. Sådanne adfærdskodekser og certificeringsordninger er "kun" vedtaget med henblik på at bidrage til korrekt anvendelse af databeskyttelsesforordningen og til at påvise, at dataansvarliges og databehandleres behandlingsaktiviteter overholder databeskyttelsesforordningen.

Et eksempel herpå er "EU Data Protection Code of Conduct for Cloud Service Providers", der for nuværende ikke kan anvendes som overførselsgrundlag.

Det er derfor vigtigt at være opmærksom på, hvorvidt et adfærdskodeks eller en certificeringsordning er udarbejdet til brug for overførsel af personoplysninger til et tredjeland, og dermed kan udgøre et overførselsgrundlag.

Vejledninger

Du kan læse mere om adfærdskodekser til brug for overførsel til tredjelande i Det Europæiske Databeskyttelsesråds vejledning herom.[7] Du skal være opmærksom på, at der på tidspunktet for vejledningens udarbejdelse er tale om et udkast til en vejledning, som er sendt i offentlig høring før den endelige vedtagelse af vejledningen.

Det Europæiske Databeskyttelsesråd er desuden i gang med at udarbejde en vejledning om brugen af certificering som overførselsgrundlag.

4.5 Retligt bindende instrumenter mellem offentlige myndigheder mv.

Hvis du er en offentlig myndighed, kan du 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.

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. Det Europæiske Databeskyttelsesråd har ligeledes udarbejdet en liste over de garantier, der som minimum skal medtages i instrumentet.

Vejledninger

Du kan finde ovennævnte anbefalinger og liste over minimumsgarantier i Det Europæiske Databeskyttelsesråds vejledning om overførsel mellem offentlige myndigheder i og uden for EU/EØS.[8]

[7] https://edpb.europa.eu/system/files/2021-07/edpb_guidelinescodesconducttransfers_publicconsultation_en.pdf
[8] https://edpb.europa.eu/system/files/2021-06/edpb_guidelines_202002_art64guidelines_internationaltransferspublicbodies_v2_da.pdf

4.6 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 en administrativ ordning, som omfatter effektive rettigheder, som 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. Det Europæiske Databeskyttelsesrådet har ligeledes udarbejdet en liste over de garantier, der som minimum skal medtages i en sådan administrativ ordning.

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

Du kan finde ovennævnte anbefalinger og liste over minimumsgarantier i Det Europæiske Databeskyttelsesråds vejledning om retligt bindende instrumenter og administrative ordninger.[9]

[9] https://edpb.europa.eu/system/files/2021-06/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v2_da.pdf

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 usikkert tredjeland.

5.1 Opfyldelse af oplysningspligten

Når du som dataansvarlig vil overføre personoplysninger til et tredjeland, får det betydning for din opfyldelse af oplysningspligten. Det gælder både, når du indsamler oplysningerne direkte hos den registrerede, og når du indsamler oplysningerne hos andre.

Hvis Europa-Kommissionen ikke har truffet en tilstrækkelighedsafgørelse, skal du således oplyse den registrerede om, hvilke tredjelande personoplysningerne vil blive overført til, og hvilket overførselsgrundlag du konkret anvender. Det gælder også, hvis du eksempelvis benytter dig af en cloud-løsning, hvor personoplysninger kan blive overført til en række tredjelande.

Du kan læse mere om oplysningspligten i Datatilsynets vejledning om registreredes rettigheder.[10] Vejledningen beskriver bl.a., hvordan og hvornår du skal give oplysningerne til den regi- strerede.

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

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"

5.2 Behandlingssikkerhed

Reglerne om behandlingssikkerhed i databeskyttelsesforordningen handler overordnet set om, at du som dataansvarlig 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.

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

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. Du kan til brug for udarbejdelsen af din risikovurdering læse Datatilsynets vejledende tekst herom. Der er som udgangspunkt ingen krav til den metode, du anvender ved udarbejdelsen af din risikovurdering, men du kan med fordel anvende den fremgangsmåde, som er beskrevet i Datatilsynets vejledende tekst om risikovurderinger. Det er vigtigt, at du dokumenterer, hvilke overvejelser og beslutninger du har gjort dig, og at du vil kunne redegøre for disse efterfølgende.

Den risikovurdering, som du foretager, skal benyttes til at fastlægge, hvilket niveau af behandlingssikkerhed du skal sikre, at din databehandler overholder. Konkret er det udtryk for en vurdering af, hvilke eventuelle yderligere sikkerhedsforanstaltninger der er behov for, når den konkrete behandling skal foretages i et tredjeland. Der er ikke her tale om en vurdering, der sigter mod at fastlægge, hvorvidt du lovligt kan overføre personoplysninger til et tredjeland, herunder om forholdene i et tredjeland griber forstyrrende ind i dit valgte overførselsgrundlag. Denne vurdering, som også populært betegnes som en ”transfer impact assessment (TIA)”, kan du læse om i afsnit 5.3.

Vejledninger

Du kan læse mere om kravene til behandlingssikkerhed i Datatilsynets og Justitsministeriets ”Vejledning om behandlingssikkerhed og databeskyttelse gennem design og standardindstillinger”[11].

Du kan læse mere om risikovurderinger i Datatilsynets og Rådet for Digital Sikkerheds ”Vejledende tekst om risikovurdering”[12].

5.3 Schrems II-afgørelsen

EU-Domstolen afsagde den 16. juli 2020 dom i den såkaldte Schrems II-sag[13].

EU-Domstolen erklærede ”Privacy Shield”-ordningen ugyldig, fordi amerikansk lovgivning ikke sætter tilstrækkelige rammer for de amerikanske myndigheders adgang til personoplysninger, som overføres til USA. Privacy Shield-ordningen var baseret på en tilstrækkelighedsafgørelse fra Europa-Kommissionen, der gjorde det muligt at overføre personoplysninger til USA, når dataimportøren havde tilsluttet sig ordningen.

EU-Domstolen fastslog endvidere, at Europa-Kommissionens standardbestemmelser som udgangspunkt fortsat kan anvendes ved overførsler til usikre tredjelande, men at dataeksportøren er forpligtet til at sikre sig, at beskyttelsesniveauet i tredjelandet i det væsentlige svarer til det, som vi har i EU. Ved vurderingen vil det eksempelvis være relevant at kigge på lovgivning

[11] https://www.datatilsynet.dk/Media/7/C/Behandlingssikkerhed%20og%20databeskyttelse%20gennem%20design%20og%20standardindstillinger%20(2).pdf

[12] https://www.datatilsynet.dk/Media/4/8/Risikovurdering.pdf

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

og praksis i tredjelandet, herunder myndighedernes (f.eks. efterretningstjenesternes) muligheder for at få adgang til personoplysninger, kontrollen hermed og de registreredes klagemuligheder. Det Europæiske Databeskyttelsesråd har udarbejdet anbefalinger om de europæiske væsentlige overvågningsgarantier, som kan være til hjælp, når man skal foretage denne vurdering.

Det afgørende er, at forholdene i tredjelandet sikrer, at beskyttelsen af de personoplysninger, som man ønsker at overføre, ikke undermineres af forholdene i tredjelandet. Hvis det ikke er tilfældet, skal dataeksportøren sørge for supplerende foranstaltninger, der afhjælper eventuelle utilstrækkeligheder i beskyttelsesniveauet.

På baggrund af dommen har Det Europæiske Databeskyttelsesråd udarbejdet anbefalinger om supplerende foranstaltninger.

Det Europæiske Databeskyttelsesråds anbefalinger om supplerende foranstaltninger er opbygget som en "køreplan", der angiver, hvilke skridt man som dataeksportør skal foretage med henblik på at vurdere, om der er behov for at sørge for supplerende foranstaltninger, når man overfører personoplysninger til et usikkert tredjeland. Det følger af anbefalingerne, at du som dataeksportør som det første bør sikre dig et grundigt overblik over dine overførsler ved bl.a. at registrere og kortlægge dem. Dernæst bør du kortlægge, hvilke overførselsgrundlag du benytter.

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. Det vil ikke være tilfældet, hvis dataimportøren på grund af lovgivningen og/eller praksis i tredjelandet, der finder anvendelse på overførslen, er forhindret i at opfylde sine forpligtelser i henhold til det valgte overførselsgrundlag.

Det vil især i følgende situationer være relevant at undersøge praksis:

1) Når et tredjelands lovgivning formelt lever op til EU's standarder, men i praksis ikke efterleves af myndighederne i tredjelandet.
2) Når lovgivningen i et tredjeland er mangelfuld, og praksis i tredjelandet er uforenelig med de forpligtelser, der er fastsat i det valgte overførselsgrundlag.
3) Når overførslen eller dataimportøren er omfattet af problematisk lovgivning i tredjelande.

Det vil i de fleste tilfælde være naturligt, hvis du som dataeksportør inddrager dataimportøren i tredjelandet, 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 mv. 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[14].

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, skal du sørge for passende supplerende foranstaltninger for at imødegå dette.

I anbefalingerne 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

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

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.

Du bør være opmærksom på, at det ikke i alle tilfælde vil være muligt at fastsætte supplerende foranstaltninger, der gør det muligt lovligt at overføre personoplysninger til et tredjeland.

Eksempel 11

Eksempel på vurdering af forhold i et tredjeland

En konsulentvirksomhed ønsker at overføre personoplysninger til en hosting service - udbyder i et usikkert tredjeland.

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 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) Undlade at overføre personoplysninger

2) Sørge for passende supplerende foranstaltninger, der sammen med overførselsgrundlaget sikrer et beskyttelsesniveau, som i det væsentlige svarer til niveauet i EU/EØS

Vejledninger

Du kan læse mere om supplerende foranstaltninger i Det Europæiske Databeskyttelsesråds anbefalinger herom[15].

[15] https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf

Du kan læse mere om de europæiske væsentlige garantier for overvågningsforanstaltninger i Det Europæiske Databeskyttelsesråds anbefalinger herom.[16]

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 af dataeksportøren eller give denne påbud om at suspendere overførslen af oplysninger. Afhængigt af omstændighederne i den enkelte sag kan det også komme på tale, at Datatilsynet politianmelder dataeksportøren.

[16] https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_da

6. Er der tale om en helt 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 som nævnt i afsnit 4.

Det gælder, hvis en af de særlige undtagelser, som er nævnt 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 generelt 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 det vil være i strid med undtagelsernes karakter.

De følgende afsnit beskriver kort de særlige situationer, hvor du kan overføre personoplysninger til et tredjeland. Du kan også læse mere om de særlige situationer i Det Europæiske Databeskyttelsesråds vejledning herom. Vejledningen indeholder en mere detaljeret gennemgang af undtagelserne. Du kan finde vejledningen på Datatilsynets hjemmeside[17].

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 kan læse mere om, hvad der er et gyldigt samtykke, i Datatilsynets vejledning om samtykke[18]. Du kan også læse nærmere om brugen af samtykke i Det Europæiske Data- beskyttelsesråds vejledning om samtykke.[19].

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.

[17] https://www.datatilsynet.dk/media/6870/edpb_guidelines_2_2018_derogations_da.pdf

[18] https://www.datatilsynet.dk/Media/0/C/Samtykke%20(3).pdf

[19] https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_da.pdf

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.

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 den sidste undtagelse kan du overføre oplysninger til et tredjeland, hvis overførslen er nødvendig af hensyn til vægtige legitime interesser, som du som dataansvarlig forfølger. Det er kun muligt, hvis den registreredes interesser eller rettigheder ikke går forud for dine vægtige legitime interesser. Det er et krav, at du foretager en vurdering af alle omstændigheder i forbindelse med overførslen og på den baggrund kan sikre passende garantier for beskyttelse af personoplysningerne, som du vil overføre.

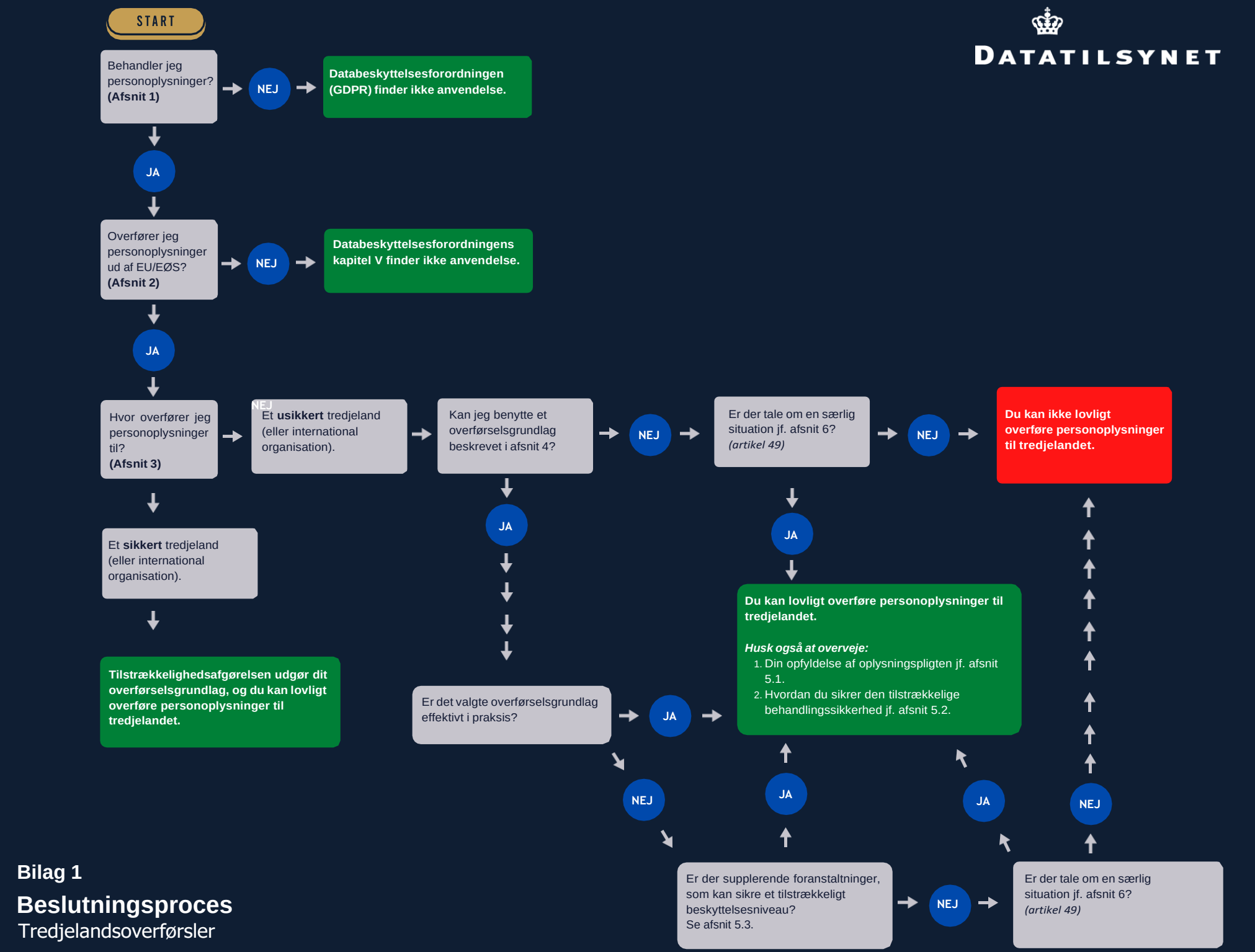
Du skal være opmærksom på, at du kun kan bruge undtagelsen i enkeltstående tilfælde dvs. hvor overførslen ikke gentages, og bl.a. kun hvis der er tale om et begrænset antal registrerede. Derudover kan du kun bruge undtagelsen, hvis du ikke kan anvende de øvrige undtagelser.

Ud over de nævnte betingelser er det et krav, at du underretter den kompetente tilsynsmyndighed om overførslen, og at du underretter den registrerede om de vægtige interesser, som begrunder overførslen.

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.

7. Bilag

Bilag 1: Et flowchart, der illustrerer beslutningsprocessen ved en tredjelandsoverførsel.
Bilag 2: Et skema med overførselsværktøjer.



Bilag 1

Beslutningsproces

Tredjelandsoverførsler

Overførselsgrundlag	Målgruppe	Ulemper	Fordele
Standardbestemmelser	Både offentlige myndigheder og private virksomheder	• Begrænset mulighed for at foretage ændringer.	• Intet krav om godkendelse fra Datatilsynet. • Kan anvendes i de fleste overførselssituationer, og de enkelte moduler kan kombineres, så aftalen dækker flere overførselssituationer. • Der kan løbende tilføjes/fjernes parter. • Må gerne indarbejdes i databehandleraftale/hovedaftalen, så man kan nøjes med ét samlet aftaledokument.
Ad hoc kontrakt	Både 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, hvilket især er relevant, hvor man ønsker at fravige standardbestemmelserne.
Bindende virksomhedsregler	Større koncerner mv.	• Skal godkendes af Datatilsynet og EDPB. • Kan være ressourcekrævende at udarbejde. • Kan kun anvendes internt i koncernen.	• Kan dække alle overførsler internt i en koncern. • Kan indgå som del af koncernens samlede compliance set-up.
Retlig bindende instrument	Offentlige myndigheder	• Kan være ressourcekrævende at udarbejde.	• Intet krav om godkendelse fra Datatilsynet. • Kan dække alle overførsler mellem de involverede myndigheder.
Administrative ordninger	Offentlige myndigheder	• Skal godkendes af Datatilsynet og EDPB.	• Kan dække alle overførsler mellem de involverede myndigheder.

Vejledning
Overførsel af personoplysninger til
tredjelande (3. udgave)

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

Foto: Colourbox

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