Dansk persondataret

Bent Ole Gram Mortensen (red.)

Dansk persondataret

Ex Tuto
PUBLISHING
www.extuto.com

Bent Ole Gram Mortensen (red.), Carina Risvig Hamer, Daniel Hartfield-Traun, Lisa Hjerrild, Kent Kristensen, Jesper Kruse Markvart, Helene Arensbak Mørk, Jesper Løffler Nielsen, Ayo Næsborg-Andersen, Sten Schaumburg-Müller, Christian Højer Schjøler, Peter Starup, Jøren Ullits & Frederik Waage
Dansk persondataret
Første udgave, første oplag

Denne bog er udgivet i januar 2020 af Ex Tuto Publishing A/S. Grafisk tilrettelæggelse og sats af mere.info A/S, som har anvendt LibreOffice/Linux samt skrifterne Baskerville Original og Cronos designet af henholdsvis František Štorm i 2000 og Robert Slimbach i 1996. Jan Trzaskowski har stået for forlagsredaktion og Tove Møgelvang-Hansen har været ansvarlig for korrekturlæsning. Bogen er trykt på Munken Pure 100 g/m^2 af Narayana Press, der ligger på Gyllingnæs syd for Odder. Indbindingen er udført af Buchbinderei S.R. Büge GmbH i Celle. Bogen er fagfællebedømt.

Ex Tuto A/S er medlem af Forening for Boghaandværk, og vi støtter bæredygtig skovforvaltning ved at anvende FSC-certificeret papir.

Copyright © 2020 the editor and the authors
Printed in Denmark 2020
ISBN 978-87-420-0033-5

Ex Tuto Publishing A/S
Toldbodgade 55, 1.
DK-1253 København K
www.extuto.com

MIX
Papir fra ansvarlige kilder
FSC® C010651
www.fsc.org

Udgivet med støtte fra
dreyersfond

FairPublishing

Kapiteloversigt

Kapitel 15

Tredjelandsoverførsler

Jesper Løffler Nielsen & Helene Arensbak Mørk

15.1. Introduktion

Strømmen af personoplysninger til og fra lande og organisationer uden for EU er nødvendig af hensyn til udbygningen af den internationale samhandel og det internationale samarbejde. Dette kan dog give anledning til udfordringer, hvad angår sikkerhed og beskyttelsen af personoplysninger, idet der er store forskelle på databeskyttelsesreglerne i lande uden for EU.

Reglerne i databeskyttelsesforordningen (GDPR) er baseret på et grundlæggende princip om fri bevægelighed af personoplysninger *inden for EU*, hvorimod nogle særlige betingelser skal være opfyldt, når oplysningerne overføres til lande *uden for EU*. Reglerne, der gennemgås i dette kapitel, har til formål at sikre, at det beskyttelsesniveau, der fremgår af GDPR (og som er gældende indenfor EU), ikke undermineres ved overførsel af personoplysninger til lande, som ikke er underlagt reglerne.[1]

Det er vigtigt at være opmærksom på, at reglerne om tredjelandsoverførsler udgør et selvstændigt krav, som kommer oven i de øvrige krav i forordningen, herunder kravet om et lovligt behandlingsgrundlag (se nærmere herom i kapitel 6). Her kan man hurtigt forledes til at

1. GDPR præambelbetragtning nr. 101.

konkludere, at man som dataansvarlig eller databehandler ikke er underlagt disse særlige krav, idet man alene udøver virksomhed inden for EU. Men som det vil fremgå af det følgende, har reglerne et overraskende bredt anvendelsesområde i praksis, bl.a. fordi det i sig selv vil bringe reglerne i spil, såfremt oplysningerne rent teknisk befinder sig på en server uden for EU.

Kapitlet har følgende opbygning: I afsnit 15.2 gennemgås forordningens geografiske anvendelsesområde, herunder etableringsbegrebet. I afsnit 15.3 forklares det, hvad det vil sige at overføre til et tredjeland. I afsnit 15.4 gennemgås de lovlige overførselsgrundlag, og i afsnit 15.5 de fire essentielle europæiske garantier. Slutteligt vil der i afsnit 15.6 blive set på anvendelsen af reglerne i praksis.

15.2. Forordningens geografiske anvendelsesområde

Forinden reglerne om tredjelandsoverførsler uddybes, er det relevant at forstå udgangspunktet; Databeskyttelsesforordningen er et EU-regelsæt, som finder anvendelse i EU.[2] Dette fremgår af forordningens artikel 3, som opstiller tre situationer, hvor reglerne vil finde anvendelse, hvoraf særligt to har praktisk relevans:

For det første vil reglerne finde anvendelse, hvis behandlingen af personoplysninger udføres for en dataansvarlig eller en databehandler, der er *etableret* i EU (afsnit 15.2.1.).

For det andet vil forordningen finde anvendelse, hvis behandlingen udføres for en dataansvarlig eller databehandler, der *ikke* er etableret i EU, hvis behandlingen omhandler udbud af varer eller tjenester til eller overvågning af registrerede i EU (afsnit 5.2.2.).

15.2.1. Etableret indenfor EU

En dataansvarlig eller databehandler er etableret indenfor EU, hvis der foretages en "effektiv og faktisk udøvelse af aktivitet gennem en mere permanent struktur".[3]

EU-Domstolen har i en afgørelse slået fast, at "enhver, selv minimal, reel og faktisk aktivitet, der udøves gennem en mere permanent

2. Rent faktisk gælder GDPR også i tre lande udenfor EU, nemlig i de såkaldte EØS-lande, Norge, Island og Lichtenstein, jf. nærmere afsnit 3 nedenfor.
3. Jf. GDPR præambelbetragtning nr. 22.

struktur" betyder, at der er tale om en etablering.[4] Dette betyder, at der i praksis ikke skal være ret mange aktiviteter i et eller flere EU-lande, førend man anses for at være etableret inden for EU og dermed omfattet af forordningens krav.

> **Eksempel:** Det indiske firma IT-India har en enkelt medarbejder ansat til at varetage sine interesser i København. Medarbejderen arbejder fra et kontorfællesskab på Islands Brygge. IT-India er derved etableret inden for EU og skal leve op til databeskyttelsesforordningen.

15.2.2. Ikke etableret inden for EU

Hvis en dataansvarlig eller databehandler ikke er etableret inden for EU, kan reglerne alligevel finde anvendelse, hvis der er tale om udbud af varer eller tjenester til registrerede i EU.

Bestemmelsen gælder, uanset om der opkræves betaling og vil oftest finde anvendelse på nethandel. Reglen vil f.eks. finde anvendelse, hvis en virksomhed markedsfører sig på et sprog, der anvendes inden for EU og almindeligt i virksomhedens hjemland, vil det være nok til at blive omfattet af reglen.[5] Sprog er dog ikke det eneste afgørende kriterium, idet man må foretage en samlet vurdering af, hvorvidt den pågældende hjemmeside kan anses for at være "rettet mod" et eller flere EU-lande.[6]

Derudover vil forordningen finde anvendelse, når der er tale om overvågning af registreredes adfærd i EU, for så vidt deres adfærd finder sted inden for EU.

> **Eksempel 1:** Det lokale australske firma Ready to Move sælger actionfigurer via en webshop. De har ingen medarbejdere eller filialer i Europa. De vil gerne udvide deres marked og har hørt, at franskmænd er glade for actionfigurer. Derfor opretter de en fransk version af deres hjemmeside, som tilgås via top-level domænet ".fr" og med anførelse af priser i euro. Ud fra en samlet vurdering må

4. EU-domstolens dom af 1. oktober 2015, *Weltimmo*, C-230-14, præmis 31.
5. Præambelbetragtning 23.
6. For en uddybning af, hvornår en hjemmeside kan anses for at være "rettet mod" et land, se Løffler Nielsen 2017, s. 187 ff.

hjemmesiden anses for at være rettet mod det franske marked, og Ready to Move skal derfor overholde forordningen.

Eksempel 2: Et firma i Panama udbyder en app, der via telefonens GPS tracker alle appens brugere og sender disse oplysninger tilbage til Panama. Fordi borgere i EU vil blive overvåget, hvis de downloader appen, skal firmaet i Panama overholde forordningen.

15.3. Hvornår er der tale om en overførsel til et tredjeland?

Et tredjeland er et land, der hverken er medlem af EU eller det Europæiske Økonomiske Samarbejde (EØS). EØS består af alle EU's medlemslande samt Island, Liechtenstein og Norge.

Der er tale om en tredjelandsoverførsel, når en dataansvarlig eller databehandler, der er etableret i EU, overfører personoplysninger til en dataansvarlig eller databehandler i et land uden for EØS.

Begrebet "overførsel" anvendes i forordningens kapitel V (artikel 44-50) vedrørende overførsel til tredjelande, men begrebets indhold er ikke direkte defineret i forordningen. Det ligger dog fast, at der er tale om en overførsel, når (1) oplysningerne rent teknisk befinder sig på en server uden for EU, (2) oplysningerne kan tilgås fra lande uden for EU,[7] eller (3) oplysningerne direkte sendes til bestemte modtagere uden for EU, f.eks. via e-mail.

Eksempel: It-supportvirksomheden WeHelpYou har kontor i Nigeria. Herfra har de som databehandler direkte adgang til at se ind i databaserne hos et dansk privathospital, herunder patientjournaler mv. WeHelpYou har til opgave at sikre, at systemet fungerer korrekt, og hjælpe med at rette eventuelle fejl og give support. Her er der tale om en overførsel til et tredjeland, og de særlige betingelser uddybet i næste afsnit skal derfor opfyldes.

7. Datatilsynet har i en afgørelse slået fast, at en såkaldt se-adgang til personoplysninger er nok til, at der er tale om en overførsel. Det har ingen betydning, om der er redigeringsret, jf. Datatilsynets afgørelse af 10. maj 2007 vedrørende Spørgsmål om krigsreglen i forhold til databehandler i tredjeland, j.nr. 2007-214-0004.

15.4. Lovlige overførselsgrundlag

Såfremt man som dataansvarlig overfører oplysninger til et tredjeland, jf. forrige afsnit, er man forpligtet til at sikre, at overførslen er lovlig.

Forordningens artikel 44-49 opstiller en række lovlige overførselsgrundlag, som overordnet kan opdeles i tre grupper: "sikre tredjelande", "fornødne garantier" og "singulære overførselsgrundlag". De tre grupper uddybes hver for sig i det følgende.

15.4.1. Sikre tredjelande (artikel 45)

GDPR artikel 45 slår fast, at man frit kan overføre personoplysninger til et tredjeland, som kan betegnes som "sikkert". Det er EU-Kommissionen, som afgør, hvilke lande der udgør sikre tredjelande.

15.4.1.1. Lande godkendt af EU-Kommissionen

På EU-Kommissionens hjemmeside kan man se en liste over, hvilke lande der er blevet godkendt som sikre tredjelande. I skrivende stund, primo 2019, er der tale om Andorra, Argentina, Færøerne, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Schweiz, Uruguay og Japan.

Der er hertil en række lande, som er underlagt særlige regler; Australien er udelukkende godkendt som sikkert tredjeland, når der er tale om overførsel af oplysninger om flypassagerer. Canada er kun godkendt som sikkert tredjeland, når modtageren af oplysningerne er underlagt den canadiske Personal Information Protection and Electronic Documents Act (PIPED ACT). Også for USA gælder særlige regler, som kort gennemgås i det følgende.

15.4.1.2. Særligt om USA (Privacy Shield)

Selvom de fleste af verdens store tech-giganter er hjemmehørende i USA, er landet ikke godkendt som et sikkert tredjeland. Landet har imidlertid meget stor betydning for de data, der hver dag udveksles via internettet, hvorfor USA og EU har indgået en særlig politisk aftale kaldet "Privacy Shield". Amerikanske virksomheder/organisationer kan tilmelde sig ordningen via det amerikanske handelsministerium. En liste over certificerede virksomheder kan findes på <www.privacyshield.gov/list>.

Hvis en amerikansk virksomhed/organisation er tilmeldt Privacy Shield-ordningen og er certificeret under den, kan en dataansvarlig eller databehandler inden for EU lovligt overføre personoplysninger til disse virksomheder uden andet overførselsgrundlag.

Man har tidligere haft en lignende ordning kaldt Safe Harbor. Denne ordning blev imidlertid underkendt af EU-Domstolen på grund af utilstrækkelig sikkerhed.[8] Forskellene mellem Privacy Shield og Safe Harbor er ikke mange. Der verserer lige nu en sag vedrørende Privacy Shield, og tiden må vise, om også denne ordning bliver underkendt.

15.4.2. Fornødne garantier (artikel 46 og 47)

Usikre tredjelande er lande uden for EØS, der ikke er godkendt som sikre tredjelande. For lovligt at overføre til et usikkert tredjeland skal man have et overførselsgrundlag, som ifølge artikel 46 opfylder de fornødne garantier for databeskyttelse:

- Retligt bindende instrument
- Bindende virksomhedsregler
- Adfærdskodekser og certificeringsmekanismer
- Standardbestemmelser
- Ad hoc-kontrakter

Fire af de fem gyldige overførselsgrundlag gennemgås i det følgende. Adfærdskodekser og certificeringsmekanismer vil ikke blive gennemgået yderligere.

15.4.2.1. Retligt bindende instrument (offentlige myndigheder og organer)

Der er mulighed for at overføre personoplysninger imellem offentlige myndigheder med grundlag i et såkaldt retligt bindende instrument, jf. artikel 46, stk. 2, litra a.

Et retligt bindende instrument kan eksempelvis være en udvekslingsaftale på skatteområdet. Hvis Skatteministeriet i Danmark f.eks.

8. Sag C-362/14, *Schrems*.

har indgået en udvekslingsaftale med myndighederne i Tyrkiet, vil det være lovligt at overføre personoplysninger hertil.[9]

15.4.2.2. Bindende virksomhedsregler (koncerner)

Bindende virksomhedsregler (engelsk: "Binding Corporate Rules") er regler, som fastlægges internt i en koncern, og som sikrer lovlig overførsel imellem de forskellige selskaber i koncernen, jf. artikel 46, stk. 2, litra b, og artikel 47, stk. 1. Det er uden betydning, hvor små eller store de forskellige selskaber i koncernen er.

Hvis man benytter bindende virksomhedsregler, kræves der ikke specifik godkendelse til de enkelte tredjelandsoverførsler til andre dele af koncernen, men virksomhedsreglerne skal som helhed godkendes af en kompetent tilsynsmyndighed, f.eks. Datatilsynet i Danmark.

Bindende virksomhedsregler udgør alene et gyldigt overførselsgrundlag *inden for samme koncern*. Det er således ikke et gyldigt overførselsgrundlag til andre uden for koncernen.

> **Eksempel 1:** Konglomeratet Zeidler har selskaber i 30 forskellige lande. Hovedkontoret ligger i København, hvorfra der skal sendes oplysninger om samarbejdspartnere til et datterselskab i Sydafrika. Zeidler er en koncern, så hvis de har udarbejdet bindende virksomhedsregler, som er godkendt af Datatilsynet, kan de lovligt overføre oplysninger fra København til Sydafrika.

> **Eksempel 2:** Zeidlers datterselskab hyrer det lokale sydafrikanske it-firma Johannesburg Masters til at vedligeholde en elektronisk personaledatabase. Selvom Zeidler har udarbejdet bindende virksomhedsregler, er der tale om en ulovlig overførsel, da Johannesburg Masters ikke er en del af Zeidler-koncernen, og der skal derfor findes et andet lovligt overførselsgrundlag.

Indholdet og strukturen af de bindende virksomhedsregler afhænger af, hvilke forhold den enkelte koncern arbejder under. Det er koncernen selv, der skal lave udkastet til reglerne og sende det til godkendelse hos myndighederne.

9. Datatilsynet 2019e.

Rammerne er altså forholdsvis frie, men der er alligevel visse minimumskrav til indholdet af bindende virksomhedsregler. Følgende skal efter artikel 47, stk. 2, være beskrevet eller bestemt i virksomhedsreglerne:

- Strukturen i og kontaktoplysninger for koncernen
- Beskrivelse af overførslerne
- Reglernes retligt bindende karakter, både internt og eksternt
- Anvendelsen af de generelle databeskyttelsesprincipper
- De registreredes rettigheder
- Ansvaret ved databrud
- Overholdelse af oplysningspligt
- Intern ansvarsfordeling, herunder håndtering af/opfølgning på klager
- Procedure for kontrol med overholdelse af de bindende virksomhedsregler
- Procedure for indberetning og registrering af ændringer af reglerne og indberetning af disse ændringer til tilsynsmyndigheden
- Passende databeskyttelsesuddannelse for personale med adgang til personoplysninger

Bindende virksomhedsregler vil i praksis kun være relevante for store, internationale koncerner. For de fleste små og mellemstore koncerner vil det næppe kunne betale sig at benytte dette overførselsgrundlag.

15.4.2.3. Standardbestemmelser

Brug af standardbestemmelser (engelsk: "Model contracts") udgør et gyldigt overførselsgrundlag, jf. artikel 46, stk. 2, litra c og d.

Standardbestemmelser kan enten være vedtaget af EU-Kommissionen (litra c) eller af en tilsynsmyndighed, f.eks. Datatilsynet (litra d). Hvis de er vedtaget af en tilsynsmyndighed, skal de endvidere godkendes af EU-Kommissionen, før de må benyttes.

De typiske standardbestemmelser er EU-Kommissionens standardkontrakter. Ved brug af disse standardkontrakter kræves der ikke specifik godkendelse fra en tilsynsmyndighed. Det er dermed et let tilgængeligt værktøj at benytte.

P.t. (marts 2019) foreligger der følgende EU-standardkontrakter:

- En kontrakt som kan anvendes til udveksling mellem en EU-dataansvarlig og en *dataansvarlig* fra et tredjeland.[10]
- En kontrakt som kan anvendes til udveksling mellem en EU-dataansvarlig og en *databehandler* fra et tredjeland.[11]

Som det måske bemærkes, mangler der en standardkontrakt for den situation, hvor en *databehandler* i EU benytter en underdatabehandler uden for EØS. I denne situation kan man vælge mellem to muligheder:

1. man kan benytte standardkontrakten fra 2010 som overførselsgrundlag fra en dataansvarlig i EU til en underdatabehandler uden for EØS og dermed springe mellemleddet (databehandleren i EU) over, *eller*
2. den dataansvarlige i EU kan give fuldmagt til databehandleren i EU, så denne kan benytte standardkontrakten fra 2010 som overførselsgrundlag til underdatabehandleren uden for EØS.

Man må gerne lade standardbestemmelserne være en del af en bredere kontrakt, og det er også muligt at medtage andre bestemmelser eller yderligere garantier.

Det er dog vigtigt at have for øje, at man ikke bør ændre i ordlyden af standardbestemmelserne. Blot minimale ændringer af ordlyden kan medføre, at der ikke længere er tale om en standardkontrakt, men derimod en *ad hoc-kontrakt*, som skal godkendes af en tilsynsmyndighed, jf. afsnit 15.4.2.4. nedenfor.

Mindre ændringer i standardbestemmelserne medfører ikke, at der er tale om en ad hoc-kontrakt. Dette kan eksempelvis være mindre sproglige ændringer, hvor f.eks. "dataeksportør" og "dataimportør" udskiftes med kontraktparternes navne eller indsættelse af supplerende kommercielle bestemmelser, hvis disse hverken direkte eller indirekte har betydning for det materielle indhold af standardbestemmelserne.[12]

10. Denne kontrakt fås i to udgaver: Decision 2001/497/EC og Decision 2004/915/EC.
11. Decision 2010/87/EU.
12. Betænkning nr. 1565, s. 662.

15.4.2.4. Ad hoc-kontrakt

En ad hoc-aftale er i denne sammenhæng en kontrakt, som har et andet indhold end standardbestemmelserne. En ad hoc-kontrakt er individuelt formuleret og skal i hvert enkelt tilfælde godkendes af en kompetent tilsynsmyndighed, f.eks. Datatilsynet.

15.4.3. Singulære overførsler (artikel 49)

Hvis der ikke er tale om overførsel til et sikkert tredjeland, og hvis man ikke kan give de fornødne garantier som gennemgået i afsnit 15.3.2, kan der være mulighed for at benytte et af de konkrete/singulære overførselsgrundlag i artikel 49.

Tilsynspraksis har tidligere fastslået, at de konkrete/singulære overførselsgrundlag skal fortolkes restriktivt, og at der er visse betingelser, der skal opfyldes. Der må således ikke være tale om (1) gentagne overførsler, (2) masseoverførsler eller (3) strukturelle overførsler. Det betyder eksempelvis, at man ikke kan benytte et konkret/singulært overførselsgrundlag til lønoverførsler, fordi lønoverførsler har en systematisk karakter og i øvrigt også gentages.[13] I sådanne tilfælde må man i stedet finde det lovlige overførselsgrundlag i de *fornødne garantier* uddybet ovenfor i afsnit 15.4.2.

Forordningens artikel 49 muliggør følgende singulære overførselsgrundlag:

- Udtrykkeligt samtykke fra den/de registrerede
- Overførslen er nødvendig for opfyldelse af en aftale, som enten (1) er indgået med den registrerede eller (2) er i den registreredes interesse.[14]
- Overførslen er nødvendig af hensyn til vigtige samfundsinteresser i EU-retten eller national ret.
- Overførslen er nødvendig for, at et retskrav kan fastlægges, gøres gældende eller forsvares.

13. Datatilsynet 2019e.
14. Ligesom det er tilfældet med samtykke, kan dette konkrete overførselsgrundlag ikke benyttes af offentlige myndigheder, og ej heller til at lovliggøre koncerninterne overførsler af ansattes oplysninger, f.eks. vedrørende lønoplysninger, jf. Artikel 29-Gruppen WP 262.

- Overførslen er nødvendig for at beskytte den registrerede eller andre personers vitale interesser.
- Overførsel sker fra et offentligt informationsregister.
- Endelig kan overførslen ske med udgangspunkt i en interesseafvejning med passende garantier.

Særligt sidstnævnte regel kan være vanskelig at gennemskue og uddybes derfor særskilt i det følgende.

I forordningens artikel 49, stk. 1, sidste punktum, findes en interesseafvejningsregel, der fungerer som en slags "sidste udvej", hvis ingen af de andre overførselsgrundlag er mulige. For at man kan benytte interesseafvejningsreglen, skal en række betingelser være opfyldt:

1. Overførsel har ikke hjemmel i artikel 45 eller 46.
2. Ingen af de andre konkrete overførselsgrundlag kan benyttes.
3. Overførslen må ikke være gentagne.
4. Overførslen må kun vedrøre et begrænset antal registrerede.
5. Overførslen skal være nødvendig af hensyn til vægtige legitime interesser.
6. Den dataansvarlige har vurderet alle omstændigheder i forbindelse med overførslen.
7. Den dataansvarlige underretter tilsynsmyndigheden om overførslen.

De syv betingelser vil ikke blive gennemgået nærmere her, men det kan konstateres, at de mange krav gør det stort set umuligt at anvende reglen i praksis. Dertil kommer, at der stilles store krav til den dataansvarliges ressourceforbrug. En undersøgelse af, om der foreligger *vægtige* legitime interesser, og at *alle* omstændigheder skal vurderes, kan være en kompliceret og langvarig proces.

I praksis vil interesseafvejningsreglen formentlig kun være anvendelig for små og mellemstore virksomheder, idet større virksomheder kan forventes at indføre nogle af de generelle foranstaltninger, eksempelvis bindende virksomhedsregler.[15]

15. Artikel 29-Gruppen WP 262.

15.5. Fire essentielle europæiske garantier

I kølvandet på EU-Domstolens underkendelse af Safe Harbor-ordningen har Artikel 29-Gruppen identificeret fire essentielle garantier,[16] der fungerer som en slags minimumskrav til de tredjelande, der overføres til.

De fire essentielle garantier er:

- Myndighedens adgang til personoplysninger skal ske på grundlag af klare, præcise og tilgængelige regler.
- Myndighedernes adgang til og brug af personoplysninger skal være nødvendig og proportional.
- Der skal være en uafhængig og effektiv tilsynsmyndighed.
- Der skal være tilgængelige og effektive retsmidler for de registrerede.

Det danske datatilsyn har givet udtryk for, at hver enkelt dataansvarlig og databehandler *udover* et gyldigt overførselsgrundlag skal sikre, at overførslen lever op til disse fire essentielle garantier.[17] Datatilsynets udlægning af disse principper og deres rækkevidde er meget vidtgående, idet konsekvensen reelt er, at den enkelte dataansvarlige myndighed, virksomhed eller forening er forpligtet til at sætte sig ind i ovenstående samfundsmæssige forhold og regler for alle de lande, der overføres personoplysninger til. Det må forventes, at der kommer en nærmere afklaring om spørgsmålet inden for en overskuelig fremtid.

15.6. Anvendelse af reglerne i praksis

I det forrige afsnit er reglerne gennemgået kronologisk. I det følgende fokuseres der på reglernes praktiske betydning, herunder hvornår reglerne oftest finder anvendelse, og hvordan betingelserne kan opfyldes i et mere praktisk perspektiv.

16. Artikel 29-Gruppen WP 237.
17. Datatilsynet 2019e.

15.6.1. Internationale koncerner

Som international koncern kommer man i særlig grad til at skulle forholde sig til forordningens bestemmelser om tredjelandsoverførsler. Som tidligere nævnt vil der være tale om en tredjelandsoverførsel, hvis der overføres personoplysninger fra f.eks. et moderselskab i EU til et datterselskab i Brasilien.

Overførsler vil ikke kun finde sted i "klassiske" tilfælde, hvor man sender en e-mail eller lignende. Der vil også være tale om en tredjelandsoverførsel, hvis den dataansvarliges afdeling i f.eks. Australien har adgang til systemer med oplysninger om EU-borgere. Af systemer kan nævnes ERP, CRM, intranet, fælles drev, mv.

Til koncernintern udveksling i store internationale koncerner vil det mest oplagte overførselsgrundlag naturligvis være bindende virksomhedsregler. Er der derimod tale om en mindre koncern, som kun har afdelinger i nogle få lande, vil omkostningerne forbundet med etablering af bindende virksomhedsregler ofte være for høje. Her vil løsningen f.eks. være at lovliggøre overførslerne ved brug af EU-Kommissionens standardkontrakter eller Privacy Shield, hvis der er tale om overførsel til et koncernselskab i USA.

15.6.2. Offentliggørelse af oplysninger på en hjemmeside

Hvis personoplysninger bliver lagt offentligt ud på en hjemmeside, hvortil alle i verden har adgang, er der ikke tale om en tredjelandsoverførsel.[18] Derimod vil der være tale om en tredjelandsoverførsel, hvis kun en begrænset skare har adgang, f.eks. via et intranet.

Selvom der ikke er tale om en tredjelandsoverførsel, er der stadig yderst strenge krav til at lægge personoplysninger offentligt ud på internettet. Det skyldes, at man stadig skal overholde de grundlæggende principper for behandling af personoplysninger i artikel 5 og have en behandlingshjemmel i artikel 6-10. Det vil typisk være meget svært at retfærdiggøre offentliggørelse af personoplysninger på nettet, medmindre det er den registrerede selv, der har stået for offentliggørelsen.

18. Sag C-101/01, *Lindquist*.

15.6.3. Cloud computing

Begrebet "Cloud computing" er en fællesbetegnelse for, at data ikke er lokalt lagret på en PC, men ligger på en "sky". Ved Cloud computing lejer du typisk software, der ligger hos en hostingudbyder, f.eks. Microsoft. Nogle af de mere kendte eksempler på cloud computing er f.eks. OneDrive, Dropbox og iCloud.

Der gælder ikke særlige persondataretlige regler for cloud computing, men der vil typisk være tale om tredjelandsoverførsler, f.eks. hvis personoplysninger ligger på en server, der er hostet i USA. De største udbydere af cloud computing-tjenester har ofte allerede lovlige overførselsgrundlag på plads, herunder i form af EU-Kommissionens standardkontrakter.