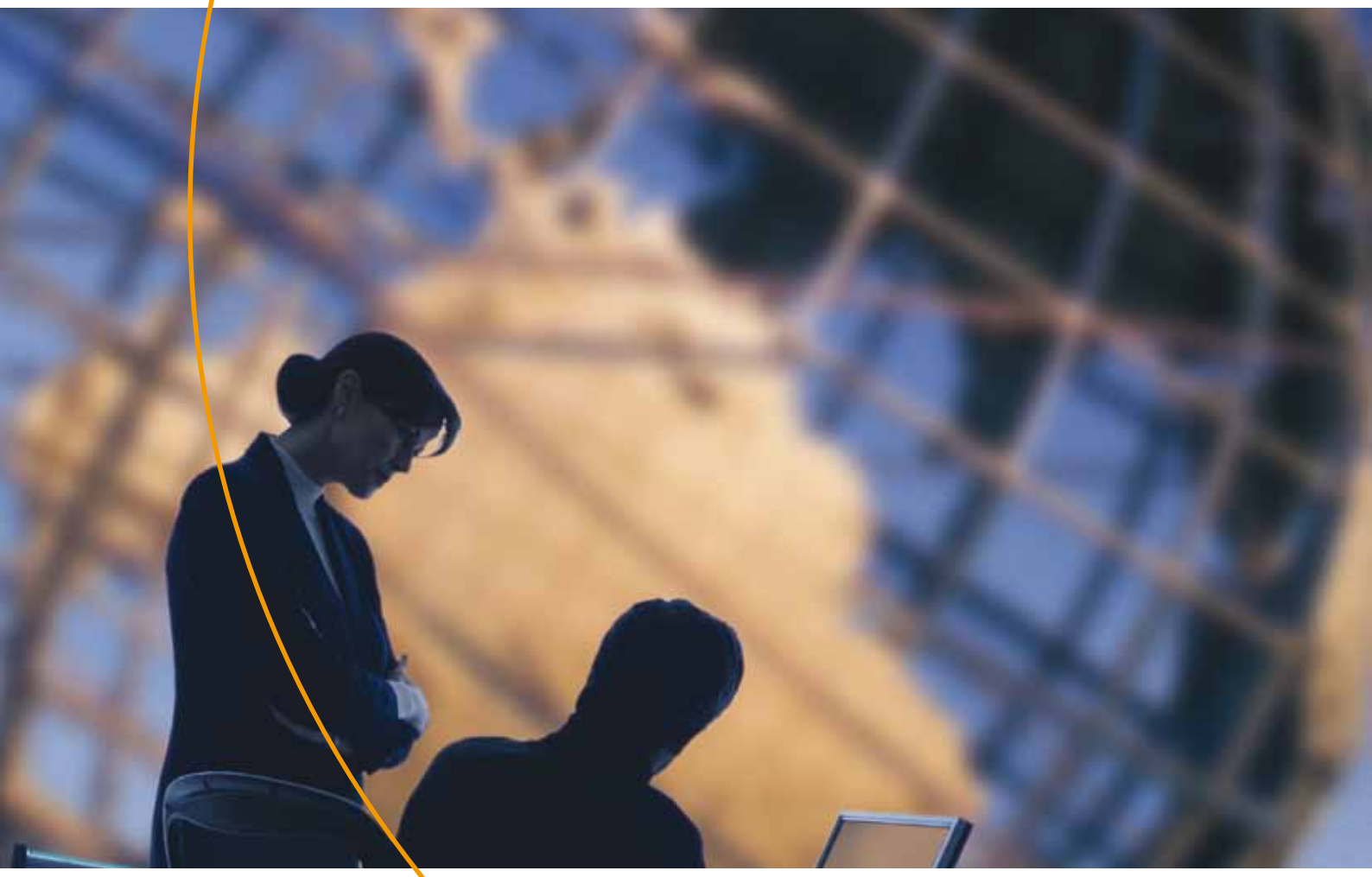
PERSONDATABESKYTTELSE

ER IKKE EN HINDRING FOR OFFSHORING AF IT



DANSK IT

PERSONDATABESKYTTELSE ER IKKE
EN HINDRING FOR OFFSHORING AF IT
Juni 2009

Forfatter:
DANSK IT's fagråd for IT og Jura ved:
Susanne Mark, Lett Advokatfirma

LETT
København Århus Kolding

DANSK IT er en it-brugerorganisation stiftet i 1958 med det formål at udbrede kendskabet til informations-teknologien og dens anvendelse, at fremme anvendelsen af it til gavn for både samfundet og den enkelte bruger af teknologien samt at samle alle it-brugere, it-professionelle og andre it-interesserede om denne opgave.

Indholdsfortegnelse

1. Indledning Side 1

2. Hvad forstås ved personoplysninger? Side 3

3. Hvornår sker der behandling af personoplysninger? Side 5

4. I hvilke tilfælde må personoplysninger overføres til et andet land? Side 6

5. Indhentelse af tilladelse hos Datatilsynet Side 10

6. Hvilke emner om personbeskyttelse bør reguleres i en offshorekontraktklausul? Side 10

7. Sammenfatning Side 12

8. Nyttige links/materiale Side 13

Bilag 1: Kommissionens standardkontraktbestemmelser Side 14

1. Indledning

I takt med at den globale konkurrence fortsat øges, overvejer mange virksomheder, om der er besparelser ved at offshore it-ydelser til lande, hvor lønomkostningerne er betydeligt lavere end i Danmark. Dette er f.eks. tilfældet i Indien og Sydafrika, hvor der yderligere er den fordel, at der kan kommunikeres på engelsk. Lønomkostningerne er også lave i nogle af de nye EU-lande, f.eks. Bulgarien, Ungarn og Rumænien.

Offshoring giver anledning til at overveje, om flytning af oplysninger til et andet land kan ske lovligt, navnlig om persondatalovgivningen gør det for besværligt at gennemføre et sådant projekt.

Datatilsynet har anlagt en bred fortolkning af, hvad der skal forstås ved at overføre oplysninger til tredjelande. Hvis en virksomhed i et tredjeland f.eks. har remote adgang til at få vist persondata, anses data for at være overført til et tredjeland. Dette gælder formentlig, selv om der ikke sker en overflytning af hardware og software.

Det er vigtigt at slå fast indledningsvist, at offshoring til et tredjeland almindeligvis kan lade sig gøre, hvis der sikres en tilstrækkelig beskyttelse af de data, som skal overføres.

I den forbindelse skal en række spørgsmål afklares. Skal offshore leverandøren have adgang til personlige oplysninger, f.eks. om kunder eller ansatte? Hvilke typer af oplysninger er der tale om? Hvorledes må offshore leverandøren håndtere disse oplysninger? Hvad er formålet? Hvordan føres der kontrol med offshore leverandørens adgang til systemerne, og hvordan sikres det, at adgangen ikke misbruges? I hvilket land er offshore leverandøren etableret? Må der ske offshoring af ydelserne til det pågældende land?

Offshoring af it-ydelser forudsætter et indgående kendskab til de konkrete it-ydelser, som skal offshores. I den juridiske analyse bør bl.a. følgende overvejes:

1. Er der tale om personoplysninger? Er det ikke tilfældet, gælder persondataloven ikke.
2. Hvis der er tale om personoplysninger, skal det overvejes, hvilket land oplysningerne overføres til.
3. Er det et EU-land eller er det et andet land, som er omfattet af en aftale med EU? Inden for EU kan overførsel af persondata ske, hvis de sædvanlige regler om behandling af persondata overholdes.
4. Uden for EU kan overførsel af persondata ske, hvis der indgås en standardkontrakt, som giver et tilstrækkeligt beskyttelsesniveau, eller hvis overførslen er omfattet af nogle særlige regler
5. En Offshorekontraktklausul bør indeholde en række bestemmelser, som tager højde for personbeskyttelse.

I det følgende uddybes, hvornår der er tale om behandling af personoplysninger, på hvilke betingelser, der må ske offshoring til andre lande, og hvilke kontraktspørgsmål som bør overvejes.

Der fokuseres på de særlige regler i persondataloven, som gælder for overførsel af personoplysninger til andre lande. De almindelige regler for behandling af personoplysninger i Danmark vil ikke blive gennemgået.

2. Hvad forstås ved personoplysninger?

En overførsel af oplysninger til en virksomhed i et andet land er omfattet af reglerne i persondataloven, hvis der er tale om personoplysninger. Er der ikke tale om personoplysninger, gælder loven ikke. I offshoring-projekter er det derfor vigtigt at få afklaret, om det er nødvendigt at overføre persondata.

I persondataloven defineres personoplysninger som 1) enhver form for information 2) om 3) en identificeret eller identificerbar 4) fysisk person (den registrerede). Der kan findes fortolkningsbidrag vedrørende dette begreb i bl.a. datatilsynets praksis og i en udtalelse af 20. juni 2007 fra den såkaldte artikel 29 gruppe (udtalelse nr. 4/2007 om begrebet personoplysninger), som bl.a. rådgiver EU institutioner. De enkelte begreber uddybes nedenfor.

1)"Enhver form for information"

Begrebet information forstås meget bredt. Alle typer af oplysninger er omfattet, herunder objektive og subjektive oplysninger, ligesom rigtige og urigtige oplysninger er omfattet. Oplysninger kan gives i hvilket som helst format eller medium, herunder i form af numre, bogstaver, billeder og lyd. Som eksempel kan nævnes videoovervågning og lydoptagelser fra et call center samt elektronisk post. Biometriske data og DNA anses også for at være personoplysninger. Biometriske teknologier kan anvendes til f.eks. fingeraftryk, håndaflæsning, irisscanning og ansigtsgenkendelse.

2) "Om"

Som udgangspunkt er oplysninger "om" en person, hvis de vedrører personen. Oplysninger kan imidlertid vedrøre både personer og ting, f.eks. prisen på et hus. Skal prisen på huset illustrere ejendomspriser i et område, er der ikke tale om personoplysninger. Skal prisen derimod anvendes til at beregne, hvor meget en person skal betale i ejendomsskat, er det en personoplysning. Tilsvarende overvejelser opstår med hensyn til bl.a. satellitdata, log af et kald fra en telefon til en anden telefon og en taxas opholdssted.

Definitionen omfatter oplysninger, som enten (1) vedrører en person (indholdselement), (2) har til formål at blive brugt om personer (formålselement) eller (3) resultatet er, at oplysninger kan få virkning for en person (resultatelement). Som eksempel kan nævnes, at selvom formålet med et satellitsystem er at afgøre, hvor hurtigt en taxa kan komme frem eller spare brændstof, vil oplysningen også kunne bruges til f.eks. at vurdere chaufførens kørsel. Dermed vil satellitdata for en taxa i visse tilfælde kunne være en personoplysning.

3) "En identificeret eller identificerbar"

En person er identificeret, hvis personen kan identificeres direkte ved navn. Udtrykket identificerbar omfatter tilfælde, hvor personen kan identificeres indirekte ved

f.eks. personnummer, telefonnummer, bilregistreringsnummer, pasnummer eller elementer, som er særlige for en persons fysiske, fysiologiske, psykiske, økonomiske, kulturelle eller sociale identitet.

Ved en vurdering af om en person er identificerbar tages der også hensyn til de midler, der med rimelighed kan tænkes bragt i anvendelse for at identificere den pågældende. I den forbindelse skal formålet med behandlingen af oplysningerne tages i betragtning. Formålet med videoovervågning af bygninger kan f.eks. være at kunne identificere personer, som begår hærværk, eventuelt ved at vise optagelserne for offentligheden. Dermed vil oplysningerne være omfattet af loven.

Et andet eksempel er dynamiske IP adresser, hvor en internetleverandør via en log registrerer dato, tid, varighed og den dynamiske IP adresse, som blev tildelt en bestemt internetbruger. Sådanne oplysninger vil ligeledes være omfattet loven.

I nogle tilfælde har en person fået et pseudonym, som oplysninger er registreret under. Pseudonymet kan være givet via en kode/nøgle. Selv om man skal kende nøglen for at kunne henføre oplysninger til en bestemt person, vil oplysningerne være omfattet af loven, hvis det er hensigten eller må forventes, at man under konkrete omstændigheder skal kunne identificere personen ved brug af nøglen, f.eks. ved kliniske test af medicin.

Hvis oplysninger er anonymiserede, således at de ikke kan identificeres, f.eks. statiske oplysninger, vil oplysningerne ikke være omfattet af loven.

4) "Fysisk person"

Det er kun oplysninger om fysiske personer, som er omfattet af loven. Det vil sige, at oplysninger om virksomheder (juridiske personer) falder uden for. Oplysninger om fysiske personer, som er ansat i virksomheden, f.eks. en persons stillingsbetegnelse og kontaktpersoner i virksomheden, anses for omfattet af begrebet personoplysninger. Dette gælder også for oplysninger om enkeltmandsejede virksomheder. I praksis vil det normalt medføre, at det er nødvendigt at overholde persondatalovens regler, når der registreres oplysninger om virksomheder.

Hvis der ikke sker behandling af personoplysninger hos offshore leverandøren, eller hvis disse oplysninger er anonymiserede, er det ikke nødvendigt at iagttage reglerne i persondataloven.

3. Hvornår sker der behandling af personoplysninger?

Begrebet ”behandling” er en række operationer ”som oplysninger gøres genstand for”. Dette forstås meget bredt, da det omfatter enhver form for håndtering af oplysninger, f.eks. (1) indsamling, registrering, systematisering, opbevaring, tilpasning, formidling, (2) enhver anden form for overladelse, sammenstilling eller samkøring samt (3) blokering, sletning eller tilintetgørelse.

Udveksling af oplysninger mellem selskaber i en koncern betragtes som videregivelse til tredjemand og er dermed omfattet af begrebet. Overladelse af oplysninger til et servicebureau og den blotte visning af oplysninger på en skærm anses også for at være en behandling.

I en konkret begrundet afgørelse har EF-domstolen dog udtalt, at der ved offentliggørelse af personoplysninger på en internetside fra EU ikke foreligger ”videregivelse til tredjeland” i den forstand udtrykket anvendes i direktivet, selv om der er adgang til oplysningerne fra et tredjeland. Afgørelsen vedrører kun tilfælde, hvor internetudbyderen er etableret i EU.

4. I hvilke tilfælde må personoplysninger overføres til et andet land?

I de tilfælde hvor offshore leverandøren skal behandle personoplysninger, er det vigtigt at slå fast, at der kan ske offshoring af personoplysninger til udlandet, hvis der findes betryggende rammer for håndteringen af oplysningerne i det andet land.

Ved analysen af et offshoring-projekt skal det først sikres, at personoplysninger behandles i overensstemmelse med persondatalovgivningen i Danmark (eksportlandet).

Dernæst bør det overvejes, om der gælder særlige regler om behandling af personoplysninger, som skal iagttages i importlandet (f.eks. Indien).

Herefter skal der tages stilling til, om personoplysninger må overføres fra Danmark til et andet land, herunder på hvilke betingelser.

a. EU-lande og EØS-lande

Personoplysninger må gerne overføres til EU-lande, f.eks. Bulgarien, Rumænien og Ungarn samt EØS-lande, f.eks. Island og Norge. Disse lande betragtes ikke som tredjelande. Udgangspunktet er, at personoplysninger frit kan overføres til disse lande.

For visse oplysninger, som har interesse for fremmede magter, gælder der særlige regler (persondatalovens § 41, stk. 4). Der kan være tale om større landsdækkende administrative systemer, f.eks. CPR og centrale skattesystemer samt oplysninger om større lastmotorkøretøjer, Sådanne oplysninger skal kunne bortskaffes eller tilintetgøres i tilfælde af krig eller lignende forhold. Reglen medfører, at behandlinger af disse oplysninger ikke må føres af en databehandler i et andet EU-land.

b. Tredjelande med tilstrækkeligt beskyttelsesniveau

Som udgangspunkt må der overføres oplysninger til et tredjeland (det vil sige et land uden for EU og EØS), såfremt der er sikret et tilstrækkeligt beskyttelsesniveau i dette land (persondatalovens § 27, stk. 1). Kommissionen har vurderet, at visse lande generelt enten via lovgivning eller via andre foranstaltninger sikrer et tilstrækkeligt beskyttelsesniveau, bl.a. Schweiz, Argentina, Canada (i begrænset omfang), Guernsey, Isle of Man og Jersey. Disse lande kan findes på Datatilsynets hjemmeside.

Der er indført en særlig ordning med USA (Safe Harbor-ordningen). Virksomheder, der har tilsluttet sig denne ordning, betragtes som virksomheder i sikre tredjelande. På Datatilsynets hjemmeside findes der et link til en liste over de virksomheder, som har tilsluttet sig ordningen.

c. Kommissionens standardkontraktbestemmelser

For lande, som ikke har et tilstrækkeligt beskyttelsesniveau, gælder, at der kan overføres data til det pågældende land, hvis der er indgået en aftale, som sikrer, at personoplysningerne behandles betryggende (persondatalovens § 27, stk. 4). Kommissionen har godkendt tre standardkontrakter:

1) *Dataansvarlig til dataansvarlig* (Kommissionens beslutning 2001/497/EF af 15. juni 2001 om standardkontraktbestemmelser for overførsel af personoplysninger til tredjelande).

2) *Dataansvarlig til dataansvarlig* (Kommissionens beslutning af 27. december 2004 om ændring af beslutning 2001/497/EF for at indføre en alternativ standardkontraktbestemmelser om overførsel af personoplysninger til tredjelande).

3) *Dataansvarlig til databehandler* (Kommissionens beslutning 2002/16/EF af 27. december 2001 om standardkontraktbestemmelser for overførsel af personoplysninger til registerførere etableret i tredjelande).

Den dataansvarlige er den virksomhed eller myndighed mv., som over for den registrerede har det umiddelbare ansvar for behandlingen af personoplysninger, og som i det daglige kan disponere over oplysningerne. Databehandleren behandler oplysninger på den dataansvarliges vegne.

De to kontrakter mellem dataansvarlige indeholder i vidt omfang ensartede bestemmelser. Formålet med kontraktbestemmelserne er at sikre, at overførte oplysninger om de registrerede undergives en betryggende behandling. Der findes derfor regler om bl.a. tekniske og organisatoriske sikkerhedsforanstaltninger, de registreredes mulighed for at håndhæve en række bestemmelser og parternes erstatningsansvar over for de registrerede samt inspektion af databehandlingsfaciliteter. En oversigt over indholdet af de respektive standardkontraktbestemmelser findes i bilag 1.

I opinion 3/2009 (WP 161, vedtaget 5. marts 2009) findes en række betragtninger fra artikel 29 gruppen vedrørende en række problemstillinger ved brug af standardkontraktbestemmelserne ”Dataansvarlig til databehandler” i forbindelse med ”global outsourcing”, herunder brug af underleverandører i tredjelande.

Hvis kontraktbestemmelserne anvendes, anses de registreredes rettigheder for at være beskyttet i tilstrækkeligt omfang. I disse tilfælde efterprøver Datatilsynet kun om kontraktbestemmelserne svarer til Kommissionens standardkontrakt. Datatilsynet anbefaler, at det bekræftes, at de anvendte kontraktbestemmelser er identiske med Kommissionens standard. Afvigelser bør fremhæves, således at Datatilsynet kan tage stilling til, om afvigelserne er i strid med Kommissionens standard.

d. Bindende virksomhedsregler

Som alternativ til standardkontrakterne kan man fastsætte Bindende Virksomhedsregler, som skal gælde for en række virksomheder. Hensigten med bestemmelserne er, at der kan udarbejdes regler, som er bindende for samtlige enheder og virksomheder i en koncern. Reglerne kan således ikke anvendes som hjemmel for overførsel af oplysninger til virksomheder, som ikke er en del af koncernen. Datatilsynene i de respektive lande kan tillade, at oplysninger udveksles mellem selskaberne, herunder til lande, som ikke har et tilstrækkeligt beskyttelsesniveau, hvis reglerne er forpligtende og bindende. Fordelen er, at reglerne kan tilpasses de konkrete forhold i koncernen.

Kommissionen har vedtaget WP 133 Anbefaling 1/2007 om standardansøgning om godkendelse af Bindende Virksomhedsregler (BCR – Binding Corporate Rules) for overførsel af personoplysninger. Anbefalingen indeholder en standardansøgning for godkendelse af Bindende Virksomhedsregler, hvor der bl.a. skal afgives en række oplysninger om indholdet af reglerne (hvordan sikres det, at de ansatte og underleverandører er bundet af reglerne internt og eksternt, sanktioner ved manglende overholdelse af reglerne, uddannelse i reglerne, hvordan håndteres klager over behandlingen af personoplysninger, hvilke typer af oplysninger er der tale om, hvordan foregår dataflowet mellem selskaberne, datasikkerhed mv.).

Ansøgningen skal kun sendes til den databeskyttelsesmyndighed i EU, som virksomheden anser for at være det ledende ("lead authority"), typisk i det EU-land, hvor det europæiske hovedkvarter er beliggende. Den ledende myndighed cirkulerer ansøgningen til databeskyttelsesmyndighederne i de øvrige lande, hvor reglerne skal gælde. Ansøgningen skal godkendes i de respektive lande.

Artikel 29 gruppen har udgivet en tjekliste over, hvilke elementer og principper et sæt bindende virksomhedsregler (Binding Corporate Rules) skal indeholde (WP 153 af 24. juni 2008) og en skabelon som hjælp til strukturering af et sæt bindende virksomhedsregler (WP 154 af 24. juni 2008).

e. Undtagelser fra forbudet mod overførsel af personoplysninger til tredjelande

I nogle tilfælde kan der overføres personoplysninger til et usikkert tredjeland, selv om der ikke er indgået en standardkontrakt (persondatalovens § 27, stk. 3). Det er bl.a. tilladt, hvis

1) den registrerede har givet udtrykkeligt samtykke,

2) overførsel er nødvendig af hensyn til opfyldelsen af en aftale mellem den registrerede og den dataansvarlige eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en sådan aftale,

3) overførsel er nødvendig af hensyn til indgåelsen eller udførelsen af en aftale, der i den registreredes interesse er indgået mellem den dataansvarlige og tredjemand,

Disse undtagelser fortolkes restriktivt. En forudsætning for videregivelse til et tredjeland er, at der kan ske videregivelse inden for EU.

Samtykke fra den registrerede

Samtykket skal være frivilligt, specifikt og informeret. Den registrerede skal have oplysning om, hvilke typer af oplysninger der overføres, til hvilke formål og til hvilke tredjelande, herunder til hvem oplysningen overføres i det pågældende land. Endvidere skal der oplyses om de specifikke risici, som er forbundet med overførslen af de pågældende oplysninger til et tredjeland uden tilstrækkeligt sikkerhedsniveau.

Ved indhentelse af samtykke online kan man anvende afkrydsningsbokse, men disse må ikke være afkrydsede på forhånd.

Samtykket kan kaldes tilbage efterfølgende (persondatalovens § 38). Dermed kan en løsning, der er baseret på samtykke, være byrdefuld for virksomheden. Det antages, at tilbagekaldelsen formentlig kun har virkning for fremtidige overførsler.

Nødvendigt for opfyldelse af en indgået aftale

Nødvendighedstesten kræver, at der er en tæt og betydelig forbindelse mellem den registrerede og kontraktens formål.

Som eksempel på bestemmelsens anvendelsesområde kan nævnes rejsebureauers overførsel af personoplysninger om deres kunder til hoteller, der medvirker ved tilrettelæggelsen af de pågældende kunders rejse eller betalinger, som foretages med et internationalt kreditkort.

Nødvendigt for indgåelse og opfyldelse af aftalen der i den registreredes interesse er indgået mellem den dataansvarlige og tredjemand

Den nødvendighedstest, som er beskrevet ovenfor, finder tilsvarende anvendelse. Som eksempel kan nævnes oplysninger, som overføres for at kunne gennemføre betalingsoverførsler til eller fra et tredjeland i den registreredes interesse.

Der findes eksempler, hvor multinationale koncerner ønsker at anvende undtagelsen med henblik på at overføre oplysninger om deres ansatte fra et datterselskab til moderselskabet, f.eks. for at centralisere koncernens betalinger og personaleforvaltning. Artikel 29 gruppen vedrørende databeskyttelse mener ikke, at sådanne overførsler kan betragtes som nødvendige for opfyldelsen af en ansættelseskontrakt.

Da undtagelserne ofte giver anledning til fortolkningstvivl, vil det almindeligvis være en mere sikker fremgangsmåde at indgå standardkontrakt (eller at benytte de bindende virksomhedsregler).

5. Indhentelse af tilladelse hos Datatilsynet

Hvis personoplysninger skal overføres til et tredjeland, som ikke har et tilstrækkeligt beskyttelsesniveau, og overførslen af personoplysninger ikke er tilladt på et andet grundlag, skal Datatilsynets tilladelse indhentes. Den dataansvarlige skal sørge for, at der ydes tilstrækkelige garantier for beskyttelse af de registreredes rettigheder.

Hvis Kommissionens standardkontrakter anvendes, vil Datatilsynet kun efterprøve, om de aftalte kontraktbestemmelser med offshore leverandøren, svarer til Kommissionens standardkontraktbestemmelser.

Der skal betales et gebyr på 1.000 kr. for ansøgningen om tilladelse.

6. Hvilke emner om personbeskyttelse bør reguleres i en offshorekontraktklausul?

I forbindelser med kontraktforhandlinger mellem leverandøren og kunden om offshoring af kundens it-systemer bør følgende overvejes:

1) Hvilke typer personoplysninger er omfattet, og hvordan skal oplysningerne behandles

2) Må leverandøren offshore til en underleverandør (til et helt eller delvist ejet selskab/uafhængig underleverandør, hvad gælder ved ændring af ejerstruktur)

3) Skal der være ret til at flytte personoplysninger til et andet land (EU-lande eller tredjelande)

4) Hvilke pligter har parterne i relation til behandling af personoplysninger og hvordan fordeles parternes ansvar over for de registrerede personer, hvis persondatalovgivningen ikke overholdes,

5) Hvilke sikkerhedskrav skal overholdes

6) Hvilke kontrolforanstaltninger skal der gennemføres, eventuelt ved en uafhængig tredjemand

7) Findes der klare beskrivelser af processen for håndtering af sikkerhed og kontrol

8) Hvilke revisorerklæringer og anden dokumentation skal kunden have

9) Hvem skal afholde omkostninger til ekstern revisors kontrol af compliance

10) Krav til arbejdsforhold hos underleverandøren, tryghedsgarantier for kunden

11) Skal Kommissionens standardkontraktbestemmelser indgå i kontrakten mellem leverandøren og kunden (eller underleverandøren og kunden)

12) Hvordan håndteres underleverandørens prisændringer mv.

Kommissionens standardkontraktbestemmelser og de bindende virksomhedsregler indeholder en række temaer, som er relevante at overveje ved kontraktindgåelsen, selv om behandlingen sker i et land med et tilstrækkeligt sikkerhedsniveau. Endvidere er det vigtigt, at der indgås en back to back aftale med offshore underleverandøren.

7. Sammenfatning

Hvis der kun overføres data, som ikke vedrører personer, f.eks. anonyme statiske oplysninger, gælder loven ikke. I disse tilfælde er overførsel af data normalt ikke problematisk.

Inden for EU er overførsel af persondata tilladt, hvis de sædvanlige regler om behandling af persondata overholdes.

Uden for EU kan overførsel af persondata ske, hvis der benyttes en af de standardkontrakter, som Kommissionen har vurderet giver et tilstrækkeligt beskyttelsesniveau, bl.a. med hensyn til privatlivets fred, personers grundlæggende rettigheder og frihedsrettigheder samt udnyttelse af de tilknyttede rettigheder. Koncerner kan i stedet vælge at fastsætte bindende virksomhedsregler, som er tilpasset virksomhedens forhold. Et resume af indholdet af disse kontrakter og regler findes i bilag 1.

I visse tilfælde kan overførsler til tredjelande være omfattet af nogle særlige undtagelser i persondataloven, men i praksis vil det normalt være bedre at benytte en standardkontrakt eller fastsætte bindende virksomhedsregler.

8. Nyttige links/materiale

Datatilsynets hjemmeside www.datatilsynet.dk indeholder forskellig information om overførsel af personoplysninger til tredjelande og konkrete udtalelser (under "værd at vide").

Udtalelse nr. 4/2007 om begrebet personoplysninger findes på Kommissionens hjemmeside på følgende link:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_da.pdf

Arbejdsdokument om en ensartet fortolkning af artikel 26, stk. 1 i direktiv 95/46/EF af 24. oktober 1995:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_da.pdf

Modelkontrakterne kan findes på Kommissionens hjemmeside på følgende link:
http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm

Der findes endvidere en række udtalelser om "Bindende virksomhedsoplysninger", som er af givet af den såkaldte Artikel 29-gruppe på følgende link:
http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_en.htm

Artikel 29 gruppen har udgivet en tjekliste over hvilke elementer og principper et sæt bindende virksomhedsregler (Binding Corporate Rules) skal indeholde (WP 153 af 24. juni 2008), som kan findes via følgende link:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp153_en.pdf

Skabelon som hjælp til strukturering af et sæt bindende virksomhedsregler (WP 154 af 24. juni 2008):
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp154_en.pdf

Kommissionen udgav den 17. marts 2009 en omfattende vejledning med ofte stillede spørgsmål og svar hertil vedrørende overførsel af persondata fra EU-lande til tredjelande:
http://ec.europa.eu/justice_home/fsj/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

Peter Blume "Retlig regulering af internationale persondataoverførsler" (2006).

Peter Blume "Databeskyttelsesret" (3. udgave 2008).

Lov om behandling af personoplysninger med kommentarer af Henrik Waaben og Kristian Korfits Nielsen (2. udgave 2008).

BILAG 1
KOMMISSIONENS STANDARDKONTRAKTBESTEMMELSER
(Sammendrag)

Dataansvarlig til dataansvarlig (Kommissionens beslutning 2001/497/EF af 15. juni 2001 om standardkontraktbestemmelser for overførsel af personoplysninger til tredjelande).

Kontrakten fra 2001 regulerer bl.a. følgende emner:

1) Der gives et løfte om, at de registrerede personer kan håndhæve en række af standardkontraktens bestemmelser over for dataeksportøren og dataimportøren vedrørende betryggende behandling af de overførte oplysninger mv. (tredjemandsløfte).

2) Dataeksportøren accepterer og garanterer bl.a., at

   a. deres behandling af personoplysninger er i overensstemmelse med eksportlandets ret
   b. ved overførsel af visse oplysninger skal de registrerede informeres om, at deres oplysninger kan blive overført til et tredjeland, der ikke sikrer et tilstrækkeligt beskyttelsesniveau
   c. give de registrerede et eksemplar af standardbestemmelserne, hvis de anmoder herom
   d. behandle forespørgsler fra tilsynsmyndigheden og den registrerede om dataimportørens behandling af personoplysninger.

3) Dataimportøren accepterer og garanterer bl.a., at:

   a. behandle oplysningerne i overensstemmelse med en række nærmere specificerede obligatoriske databeskyttelsesprincipper
   b. behandle alle rimelige forespørgsler fra dataeksportøren eller de registrerede og at samarbejde med den kompetente tilsynsmyndighed
   c. lade sine databehandlingsfaciliteter underkaste inspektion
   d. give de registrerede et eksemplar af standardbestemmelserne, hvis de anmoder herom

4) Dataeksportøren og dataimportøren hæfter solidarisk over for registrerede, som har krav på erstatning som følge af en af parternes overtrædelse af standardkontrakten.

5) Parterne er enige om at henvise eventuelle tvister til mægling. Sager afgøres af domstolene i det land, hvor dataeksportøren er etableret.

6) Efter aftale med den registrerede kan en specifik tvist henvises til en voldgift (forudsat dataimportøren er etableret i et land som har ratificeret New York-konventionen).

7) Efter kontraktens ophør gælder kontraktens bestemmelser om behandling af oplysninger fortsat for de overførte oplysninger.

8) Standardkontrakten er underlagt lovgivningen i dataeksportørens etableringsland.

9) Parterne forpligter sig til ikke at ændre de aftalte standardbestemmelser.

Dataansvarlig til dataansvarlig (Kommissionens beslutning af 27. december 2004 om ændring af beslutning 2001/497/EF for at indføre en alternativ standardkontraktbestemmelser om overførsel af personoplysninger til tredjelande)

Standardkontrakten fra 2004 er mere lempelig for virksomhederne på visse punkter, bl.a. er der ikke et solidarisk ansvar for overtrædelse af kontraktens bestemmelser. Der reguleres bl.a. følgende emner:

1) Dataeksportøren skal bl.a.:

a. garantere, at personoplysninger indsamles, behandles og overføres i overensstemmelse med eksportlandets ret
b. forsøge at fastslå på passende vis, om dataimportøren er i stand til at opfylde sine forpligtelser
c. give dataimportøren kopier af eller henvise til den relevante databeskyttelseslovgivning i dataeksportørens etableringsland
d. besvare forespørgsler fra registrerede og myndigheden vedrørende dataimportørens behandling af personoplysninger mv.
e. give de registrerede og myndigheden et eksemplar af ikke fortrolige oplysninger i standardkontrakten efter anmodning

2) Dataimportøren skal bl.a.:

a. behandle oplysningerne i overensstemmelse med en række nærmere specificerede databeskyttelsesprincipper med henblik på at give den registrerede en betryggende beskyttelse
b. besvare alle rimelige forespørgsler fra dataeksportøren, de registrerede og myndigheden mv.
c. lade sine databehandlingsfaciliteter underkaste inspektion mv. efter berettiget anmodning

3) Der gives et løfte om, at de registrerede personer kan håndhæve en række af standardkontraktens bestemmelser over for dataeksportøren og dataimportøren vedrørende betryggende behandling af de overførte oplysninger mv. (tredjemandsløfte).

4) Dataeksportøren og dataimportøren indbyrdes ansvar er reguleret. De registrerede kan på baggrund af tredjemandsløftet gøre et ansvar gældende over for den af parterne, som misligholder nærmere specificerede kontraktforpligtelser.

5) Standardkontrakten er underlagt lovgivningen i dataeksportørens etableringsland med visse undtagelser.

6) Parterne accepterer at medvirke i en forligsprocedure eller mægling mv. og at rette sig efter en afgørelse fra en domstol i dataeksportørens etableringsland eller fra tilsynsmyndigheden.

7) Standardkontrakten kan bringes til ophør under nærmere specificerede omstændigheder. Ved kontraktens ophør fritages parterne ikke fra forpligtelserne med hensyn til behandlingen af de overførte oplysninger.

8) Parterne kan ikke ændre de aftalte standardbestemmelser, bortset fra ajourføring af visse oplysninger.

Bestemmelserne i de respektive kontrakter fra 2001 og 2004 kan ikke kombineres.

Hvis ansvaret for behandlingen af oplysninger ikke overføres til en anden, men der kun er tale om at få hjælp til teknisk opbevaring og bearbejdning af personoplysningerne, skal kontrakten om "registerførere" (databehandlere) anvendes.

Dataansvarlig til databehandler (Kommissionens beslutning 2002/16/EF af 27. december 2001 om standardkontraktbestemmelser for overførsel af personoplysninger til registerførere etableret i tredjelande).

Kontrakten fra 2001 mellem en dataansvarlig og en databehandler skal indeholde bestemmelser om bl.a. følgende emner:

1) Der gives et løfte om, at de registrerede personer kan håndhæve en række af standardkontraktens bestemmelser over for dataeksportøren og dataimportøren vedrørende betryggende behandling af de overførte oplysninger mv. (tredjemandsløfte).

2) *Dataeksportøren* accepterer og garanterer bl.a., at

   a. deres behandling af personoplysninger er i overensstemmelse med databeskyttelseslovgivningen i det land, hvor dataeksportøren er etableret
   b. instruere dataimportøren om kun at behandle personoplysninger på vegne af dataeksportøren i overensstemmelse med databeskyttelseslovgivningen og standardkontrakten
   c. dataimportøren tilvejebringer tilstrækkelige garantier med hensyn til nærmere fastsatte tekniske og organisatoriske sikkerhedsforanstaltninger, som skal beskytte personoplysninger mod hændelig eller ulovlig tilintetgørelse, hændeligt tab, ændring, uautoriseret videregivelse eller adgang mv., og at disse sikkerhedsforanstaltninger overholdes
   d. ved overførsel af visse oplysninger informeres de registrerede om, at deres oplysninger kan blive overført til et tredjeland, der ikke sikrer et tilstrækkeligt beskyttelsesniveau
   e. give de registrerede et eksemplar af standardbestemmelserne, hvis de anmoder herom

3) *Dataimportøren* accepterer og garanterer bl.a., at:

   a. behandle oplysningerne på vegne af dataeksportøren i overensstemmelse med dennes instrukser og standardbestemmelserne mv.
   b. den lovgivning, som dataimportøren er underlagt, ikke giver grund til at tro, at forpligtelserne ikke kan overholdes samt straks at give dataeksportøren meddelelse, hvis dette ændres
   c. iværksætte nærmere fastsatte tekniske og organisatoriske sikkerhedsforanstaltninger,
   d. underrette dataeksportøren om anmodninger om videregivelse af personoplysninger fra en retshåndhævende myndighed eller fra de registrerede samt underrette om enhver utilsigtet eller uautoriseret adgang
   e. behandle alle forespørgsler fra dataeksportøren og følge anbefalinger fra tilsynsmyndigheden
   f. lade sine databehandlingsfaciliteter underkaste inspektion
   g. give de registrerede et eksemplar af standardbestemmelserne, hvis de anmoder herom

4) Dataeksportøren skal betale erstatning til registrerede, som har lidt skade som følge af overtrædelse af kontrakten (med mulighed for regres over for dataimportøren, hvis tabet skyldes, at dataimportøren har overtrådt standardbestemmelserne). I nærmere beskrevne tilfælde kan registrerede fremsætte kravet direkte over for dataimportøren.

5) Parterne er enige om at henvise eventuelle tvister til mægling. Sager henvises til domstolene i det land, hvor dataeksportøren er etableret. Efter aftale med den registrerede kan en specifik tvist henvises til en voldgift (forudsat dataimportøren er etableret i et land som har ratificeret New York-konventionen).

6) Dataeksportøren giver tilsynsmyndigheden et eksemplar af standardbestemmelserne, hvis denne anmoder herom. Tilsynsmyndigheden har ret til at foretage inspektion hos dataimportøren.

7) Standardkontrakten er underlagt lovgivningen i dataeksportørens etableringsland.

8) Parterne forpligter sig til ikke at ændre de aftalte standardbestemmelser.

9) Ved afsluttet behandling af personoplysninger skal de overførte personoplysninger efter dataeksportørens ønske enten returneres eller destrueres.

DANSK IT'S FAGRÅD FOR IT OG JURA

Fagrådet beskæftiger sig med emner, der vedrører såvel it som jura, og som er af almen interesse. Endvidere er fagrådets formål udveksling af erfaringer og information både internt i foreningen og eksternt. Fagrådet medvirker ved udfærdigelse af DANSK IT's høringssvar, deltagelse i udvalgsarbejde om it-standardkontrakter, og forsøger endvidere at orientere om relevante juridiske tiltag bl.a. gennem konferencer, artikler og publikationer.

DANSK IT

Bredgade 25 A - 1260 København K
33 11 15 60 – www.dansk-it.dk