Danske Advokater

Aktuelle udfordringer ved brug af Cloud-tjenester

24. august 2022

Advokat, partner Michael Hopp

PLESNER

Dagens program

- Om cloud

- Aktuelle udfordringer ved brugen af cloud
  1) Screening af cloud-leverandøren og dennes underdatabehandlere
  2) Risikovurdering og eventuel konsekvensanalyse af cloud-leverandøren
  3) Cloud-leverandørens (mulige) brug af data til egne formål
  4) Tredjelandsoverførsler
     - Utilsigtede tredjelandsoverførsler

- Spørgsmål

Om cloud

Begrebet "cloud"

- Model til at tilvejebringe standardiserede it-ressourcer, typisk større decentrale samlinger af servere, der tilgås via internettet
- Kan være skræddersyede eller standardiserede
- Kendetegnende, at man som kunde alene har kontrol over typen og mængden af ressourcer, fx lagring og proceskraft, men ikke over hvilke specifikke ressourcer leverandøren tilvejebringer eller hvor disse ressourcer tilvejebringes.
- Typer af cloud:
  - Infrastruktur som en service (IaaS) -> adgang til ren infrastruktur
  - Platform som en service (PaaS) -> adgang til infrastruktur som leverandør servicerer med styresystem mv.
  - Software som en service (SaaS) -> adgang til færdigudviklede cloudbaserede forretningsapplikationer
- Privat cloud, fælles cloud, offentlig tilgængelig cloud, hybrid cloud.

Databeskyttelsesretlige udfordringer ved brugen af cloud

PLESNER

Hvad ser Datatilsynet på?

- Datatilsynets spørgeskema om tilsyn med cloudservices - 1. august 2022
  - Kend dine services
  - Kend dine leverandører
  - Tilsyn med leverandører
  - Overførsel til tredjelande

- Hvad ser DT på?
  - Evnen til at kunne redegøre for dine behandlingsaktiviteter, herunder datastrømme
  - Vurdering af leverandørens evne til at sikre, at behandlingen sker i overensstemmelse med databeskyttelsesreglerne
  - Databehandleraftalens ordlyd og gennemsigtighed
  - Databehandleraftalens afspejling af dine krav med hensyn til behandlingsaktiviteten
  - Kontroller og opfølgning på eventuelle afvigelser i forhold til det aftalte

Aktuelle udfordringer ved brug af cloud

- Screening af cloud-leverandøren og dennes underdatabehandlere
- Risikovurdering og eventuel konsekvensanalyse af cloud-leverandøren
- Cloud-leverandørens (mulige) brug af data til egne formål
- Tredjelandsoverførsler
  - Utilsigtede tredjelandsoverførsler

Husk

Hvis det ikke er dokumenteret

Så er det ikke gjort!

1. Screening af cloud-leverandøren

1. Kortlægning, kortlægning og kortlægning!

- Kend dig selv!
  - Hvilke behandlingsaktiviteter og datapunkter mv. indgår i de forretningsprocesser, som understøttes af de IT-services, som skal outsources?

- Hvilken service leverer databehandleren?
  - Hvilke ydelser (husk eventuelle tillægsydelser, f.eks. support)
  - Hvilke data?
    - Kundens data (som "overlades", dvs. lægges ind i tjenesten eller genereres ved almindelig brug)
    - Metadata om egne medarbejderes brug af tjenesten?
  - Hvilke aftalevilkår -> indeholder aftalen fx vilkår der gør, at man ikke kan leve op til sine forpligtelser
    - Sletning af data
    - Databehandlers anvendelse af kundens data til egne formål
  - Hvilke underdatabehandlere og tredjelande – hele kæden
  - Hvilken sikkerhed

1. Brug af databehandlere

- Hvad betyder det, at man udelukkende må anvende cloud-leverandører/databehandlere, der kan stille de fornødne garantier?

- Udgangspunkt
  - Egne beskrivelser/risikovurderinger

- Helt fundamentalt
  - Man må som dataansvarlig ikke acceptere hverken
    - egentlige ulovligheder eller
    - en for høj residualrisiko i forhold til de registreredes rettigheder og frihedsrettigheder,
  - blot fordi en behandling ikke længere udføres af én selv, men af en databehandler

- Man kan outsource opgaven, men ikke ansvaret!

1. Hvad kan man se på ved screening?

Art. 28(1)

Kasse 2-4 undergives løbende tilsyn

1. Databehandleraftale

- Leveres ofte af DB
- Andre vilkår, ex. "MS tillæg om databeskyttelse"?
- Andre showstoppers?

2. Overholdelse af aftalen

- Hvordan vil DB efterleve aftalen?
- Fx -> hvilke procedurer har man på plads for at sikre tavshedspligt og besvarelse af anmodninger fra registrerede

3. Behandlingssikkerhed

- Se på DB's egen sikkerhed, herunder risikovurderinger
- Hvordan imødegås identificerede risici

4. Tredjelande

- Sker der overførsler?
- Er der et overførselsgrundlag?
- Er der lavet en (lødig) TIA?

1. Screening af databehandlere

- Hvordan - Spørgeskema/screeningsværktøj
  - Se checkliste i cloud vejledning, s. 12 ff.
  - Datatilsynets spørgeskema vedr. brug af cloud tjenester
  - CFCS vejledning – Informationssikkerhed i leverandørforhold
  - Enisa - https://www.enisa.europa.eu/topics/cloud-and-big-data?
  - EIOPA - https://www.eiopa.europa.eu/content/guidelines-outsourcing-cloud-service-providers_en

- a) Er cloudleverandøren i henhold til databehandleraftalen forpligtet til alene at behandle personoplysninger efter din instruks, eller forbeholder leverandøren sig ret til at behandle oplysninger til egne formål?

- b) Har cloudleverandøren etableret politikker og procedurer, der sikrer, at leverandørens medarbejdere har forpligtet sig til fortrolighed eller er underlagt en anden passende tavshedspligt, og kan leverandøren påvise dette?

- c) Har cloudleverandøren etableret et passende niveau af behandlingssikkerhed i lyset af den overladte behandlingsaktivitet, herunder henset til ansvarsfordelingen mellem dig og leverandøren?

1. Screening af databehandlere

- d) Har cloudleverandøren en procedure for screening af eventuelle underdatabehandlere med henblik på at sikre, at underdatabehandleren også vil være i stand til at leve op til de databeskyttelseskrav, som du har fastsat over for leverandøren, og indebærer proceduren i givet fald fremsendelse af underdatabehandlerens dokumentation til dig som den dataansvarlige?

- e) Indeholder ovennævnte procedure en frist for fremsendelse af dokumentation af screening af underdatabehandleren, der stemmer overens med fristen for varsling om brugen af nye underdatabehandlere eller ændring af nuværende underdatabehandlere?

- f) Afspejler den (eventuelle) underdatabehandleraftale de samme krav, som vil blive pålagt cloudleverandøren af dig som den dataansvarlige?

- g) Har cloudleverandøren en fuldstændig oversigt over, hvilke underdatabehandlere leverandøren benytter til brug for levering af sine services, herunder hvilke lande – særligt uden for EU/EØS – disse underdatabehandlere befinder sig i, og fra hvilke lande leverandøren og eventuelle underdatabehandlere kan tilgå oplysningerne? Har cloudleverandøren, i bekræftende fald, etableret et overførselsgrundlag, der er effektivt i lyset af den behandlingsaktivitet, du overlader til leverandøren??

1. Screening af databehandlere

- h) Har cloudleverandøren – henset til den overladte behandlingsaktivitet – procedurer for at bistå dig med håndtering af anmodninger fra de registrerede efter databeskyttelsesforordningens kapitel III?

- i) Har cloudleverandøren procedurer for håndtering af brud på persondatasikkerheden, og omfatter disse procedurer i givet fald cloudleverandørens bistand til dig med din forpligtelse til at anmelde brud på persondatasikkerheden til Datatilsynet?

- j) Kan cloudleverandøren slette eller tilbagelevere personoplysningerne ved behandlingsaktivitetens ophør?

- k) Har cloudleverandøren en procedure for at bistå dig i forbindelse med dit tilsyn med vedkommende eller for gennemførelse af revision ved uafhængige tredjemænd fx revisorer?

2. Risikovurdering og eventuel konsekvensanalyse af cloud-leverandøren

2. Risikovurdering og evt. konsekvensanalyse

- **Initiel** risikovurdering af behandlingsaktiviteterne – og outsourcingen heraf
  - Hvis høj iboende risiko ved outsourcingen -> Konsekvensanalyse (art. 35)
    - Hvis konsekvensanalyse fører til høj residualrisiko -> forelæggelse for Datatilsynet
    - "*Datatilsynet lægger – ligesom Helsingør Kommune – til grund, at flere af behandlingerne indebærer en høj risiko*"
  - Hvis ikke-høj iboende risiko -> Almindelig risikovurdering (art. 25)

- Konsekvensanalyse/risikovurdering
  - Starter altid med vurdering af legalitet, jf. art. 28.1
    - F.eks. vurdering af, hvilke persondata der er nødvendige ved brugeroprettelse, samt om der er tilstrækkelig sikkerhed. Men også f.eks. tredjelandsoverførsler eller brug til egne formål.
  - Alle risikoscenarier forbundet med outsourcingen skal inkluderes i risikovurderingen
  - Residualrisko?
    - Acceptabel?
    - Hvis konsekvensanalyse med høj residualrisiko -> konsultation af Datatilsynet, jf. art. 36

2. Risikovurdering og evt. konsekvensanalyse

- **Eksempel**
  - Der er foretaget en risikovurdering vedrørende art. 5.1.e – sletning – i eksisterende system
  - Parameterstyret sletning var muligt
  - Fastsat kontrol/procedure for opfølgning på sletning
    - Se f.eks. Carlsberg afgørelsen

  - Ny SaaS løsning
    - Anden form for opsætning af parameterstyret sletning – eller måske manuel sletning
    - Ny form for såvel udførelse, som kontrol/opfølgning

  - Sammenhold med Datatilsynets spørgeskemaer, f.eks. vedrørende sletning

- **Når man benytter standardløsninger -> begrænset rum for foranstaltninger på systemsiden**

Hvad forventer Datatilsynet?

- Man skal kunne redegøre for, hvorfor de valgte foranstaltninger kan anses for passende (og for deres implementering, udførelse, tilsyn og vedligeholdelse…)

- Det kræver, at man har styr på (fra begyndelsen og over tid…)
  - Behandlingsaktivitetens indhold [se revideret vejledning om art. 30-fortegnelse]
  - Behandlingsaktivitetens lovlighed
  - Hvilke trusler, behandlingsaktiviteten kan blive ramt af
  - Hvilke skade(r), den enkelte trussel kan forårsage
  - Sandsynligheden for, at truslen materialiserer sig, og skaden indtræffer
  - Hvilke konsekvenser det vil have for de registreredes rettigheder og frihedsrettigheder, såfremt skaden indtræffer
  - Fastlæggelse af mitigerende foranstaltninger/kontroller
  - Residualrisko

3. Cloud-leverandørens (mulige) brug af data til egne formål

3. Eksempler på "andre" vilkår – brug af data til egne formål

- Databehandlerens anvendelse af kundens data = videregivelse

- Datatilsynets vejledning om cloud

> *"Hvis du ønsker at tillade leverandøren at behandle oplysninger til egne formål eller ønsker at benytte en leverandør, der forbeholder sig retten til at behandle oplysninger, som overlades til vedkommende, til egne formål, skal du være opmærksom på følgende:*
>
> *a) Formålene, hvortil leverandøren ønsker at behandle personoplysningerne, må ikke være uforenelige med de formål, hvortil oplysningerne oprindeligt blev indsamlet af dig*
>
> *b) Du skal have et retligt grundlag for at videregive personoplysningerne til leverandøren til brug for dennes behandlingsaktiviteter (ligesom leverandøren også skal identificere et retligt grundlag for sin behandling)."*

- Det afgørende er ikke, hvad databehandleren gør, men hvad databehandleren har ret (instruks) til at gøre
  - Cloud vejledning, s. 14
  - Et "forbehold" er også en instruks

3. Eksempler på "andre" vilkår – brug af data til egne formål

- Microsoft – 6 egne formål (kommercielle formål mv., samt myndighedsanmodninger fra ethvert land**)**
- AWS – 1 eget formål (myndighedsanmodninger fra ethvert land)
- OBS: Hvis en dataansvarlig ikke selv lovligt kan foretage en behandling, så kan den samme behandling heller ikke lovligt finde sted hos en databehandler!
  - Databehandleren handler alene på den dataansvarliges vegne – efter instruks
  - Alle databehandlerens behandlinger skal (a) følge af instruks, eller (b) ske for at efterleve en retlig forpligtelse i EU-retten eller national lovgivning i en EU-medlemsstat
    - Tredjelandes retlige forpligtelser anerkendes ikke inden for EU som en retlig forpligtelse
    - [Undtagelse ved behandling i et 3L i henhold til 3L lovgivning efter en (lovlig) 3L overførsel = Schrems II problemet]
- Er anvendelsen ikke lovlig -> GDPR artikel 28.1 -> Vilkåret kan ej tiltrædes (f.eks. via databehandleraftalen)

4. Tredjelandsoverførsler

Overførsel til tredjelande

UP: Overførsler til tredjelande er forbudt – GDPR art. 44

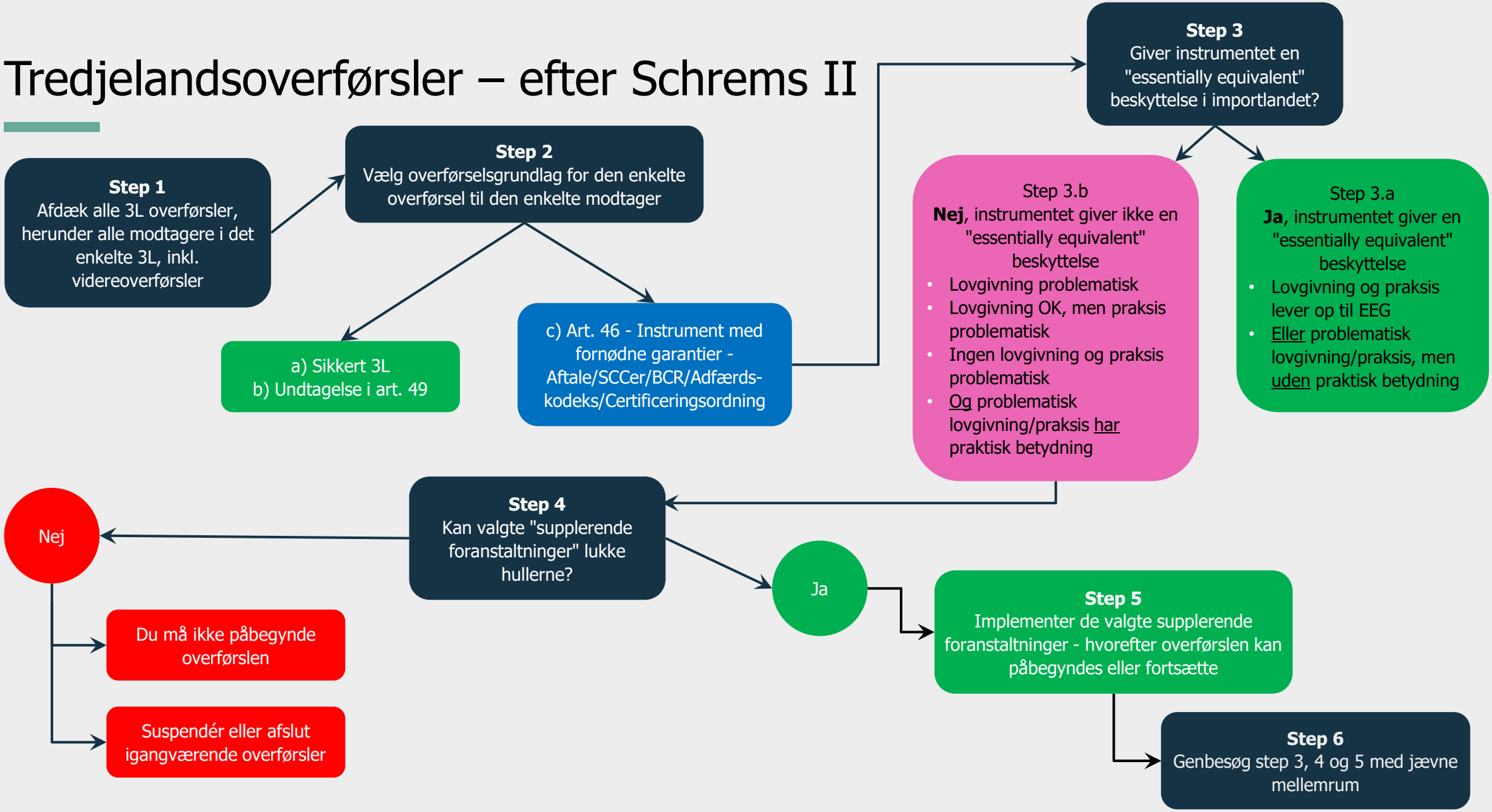
- Påhviler både dataansvarlig og databehandler
- Kan finde sted, hvis hjemmel i kapitel V samt hvis GDPR i øvrigt overholdes (dobbelt hjemmelskrav)
- Tredjelande: Lande uden for EU/EØS
  - EØS -> Norge, Island og Lichtenstein
- Hvad er en tredjelandsoverførsel?
  - Fysisk flytning (inkl. kopiering) af data til tredjeland
  - Fjernadgang fra tredjeland til data inden for EU/EØS
    - Adgang til databaser, hvor persondata kan kopieres/printes
    - Adgang til databaser, som åbnes f.eks. ved support
    - Visning af persondata på skærm (også i en Citrix løsning), f.eks. åbning/visning ved bistand til support case

- **Husk "onward transfers" -> skal også håndteres som tredjelandsoverførsel -> f.eks. deling med ny DA i US**

Step 1 - kortlægning af 3L-overførsler

- Alle overførsler i hele leverandørkæden skal identificeres!
- Hav eventuelt dialog med databehandler om hvilke underdatabehandlere, der benyttes til de valgte services
- Datatilsynets cloud vejledning, side 18
  - *"Hvis det ikke er muligt at indgå i en dialog med cloudleverandøren, eller hvis din dialog med leverandøren ikke giver dig tilstrækkelig information til, at du over for Datatilsynet vil kunne dokumentere hvilke specifikke underdatabehandlere, der er relevante for de services, du benytter, skal du efter Datatilsynets opfattelse lægge til grund, at alle de underdatabehandlere, der fremgår af cloudleverandørens generelle oversigt, benyttes til levering af dine cloudservices."*

Tredjelandsoverførsler – efter Schrems II



PLESNER

Step 2 - Overførselsgrundlag

- **U2: Tilvejebringelse af <u>fornødne garantier – GDPR art. 46</u>**
  a) Retligt bindende instrumenter, som kan håndhæves, mellem offentlige myndigheder
  b) Bindende virksomhedsregler (BCR), jf. art. 47
  c) Kommissionens standardkontraktsbestemmelser (SCC / Model Clauses)
  d) Standardkontraktsbestemmelser fra tilsynsmyndighed
  e) Adfærdskodeks/certifikat med bindende tilsagn

- Garantierne skal kompensere for manglende beskyttelse i tredjelandet

- Nye SCC den 4. juni 2021 -> modulopbygget -> generelle bestemmelser + moduler
- Gamle SCC'er udløber 27. december 2022

Schrems II dommen

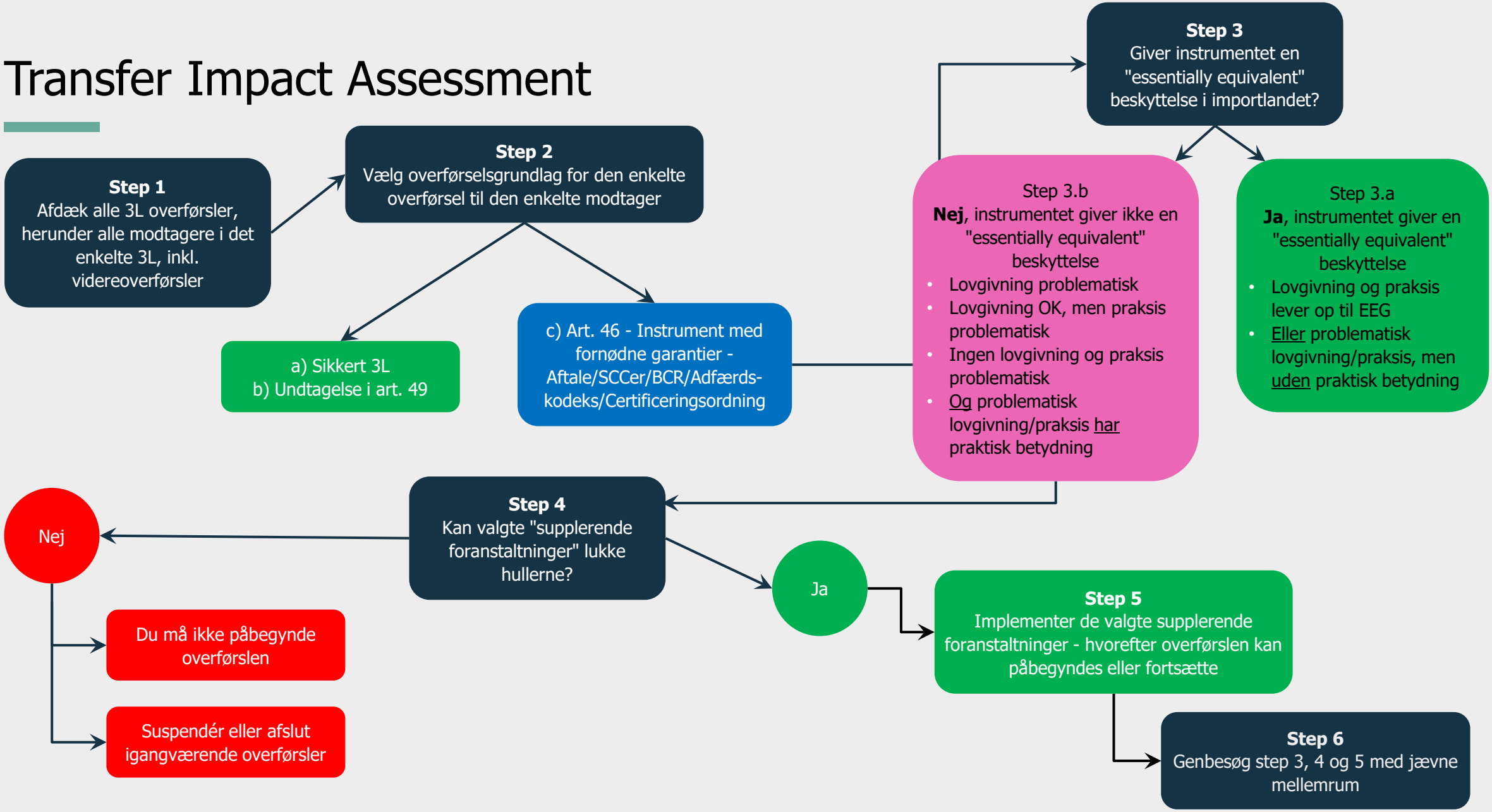
- EU-Domstolen fastslår, at SCC'er generelt er gyldige som overførselsgrundlag

- Ved sikring af tilstrækkelige garantier skal SCC'er – for så vidt angår en eventuel adgang for et tredjelands offentlige myndigheder til de overførte personoplysninger – suppleres med en konkret vurdering i forhold til de relevante forhold i tredjelandes retssystem, herunder navnlig de elementer [som følger af Charter, art. 7, 8, 52 og 47 = Essentielle Europæisk Garantier]

- Samlet beskyttelsesniveau i 3L skal i praksis være "essentially equivalent" med beskyttelsen i EU

- Hvis utilstrækkelig beskyttelse, så skal man
  - Implementere "supplerende foranstaltninger", som lukker hullerne
  - Alternativt undlade eller stoppe overførslen

Transfer Impact Assessment



PLESNER

Særligt vedrørende step 4 – supplerende foranstaltninger

- **Tekniske foranstaltninger**
  - Kryptering – både under transport og ved opbevaring
  - Pseudonymisering
  - Opbevaring af "nøgler"
- **Kontraktuelle foranstaltninger**
  - Forpligte importør til at oplyse om "access requests"
  - Styrke adgang til kontrol med importør
  - Forpligte importør til at informere om lovændringer
- **Organisatoriske foranstaltninger**
  - Fastsætte procedurer for håndtering af 3. lands overførsler (inden for koncern)
  - Fastsætte procedurer til sikring af at ikke overføres mere end højst nødvendigt

De valgte foranstaltninger skal være effektive!

- **EDPB pkt. 74**: "Selecting and implementing one or several of these measures will not necessarily and systematically ensure that your transfer meets the essential equivalence standard that EU law requires. You should select those supplementary measures that can effectively guarantee this level this level of protection for your transfers."
  - Med andre ord: Er "hullet" lukket set fra de registreredes synsvinkel?
- **EDPB pkt. 53: "**Contractual and organisational measures alone will generally not overcome access to personal data by public authorities of the third country based on problematic legislation and/or practices"
  - => Tekniske foranstaltninger vil typisk være nødvendige, for at supplerende foranstaltninger kan lukke hullet i beskyttelsen
- Hvorfor?

EDPB gennemgår en række scenarier

- Afsnit 79-92 -> scenarier hvor tekniske foranstaltninger kan være effektive i forhold til at sikre "essentially equivalence"

Eksempler:

1. Dataeksportør bruger leverandør i tredjeland til at opbevare backup, og der er ikke behov for adgang til oplysninger i klartekst
2. Overførsel af pseudonymiserede oplysninger
3. Krypterede oplysninger passerer alene igennem et tredjeland
4. Behandlinger fordelt på databehandlere i forskellige jurisdiktioner
5. Overførsel til beskyttet importør

- Fælles for eksemplerne 1-4: Dataimportør får ikke adgang til oplysninger i klartekst

- Eksempel 5: Begrænset til enkeltstående overførsler – fx til læge eller advokat

- Se DT's eksempler i Cloud vejledning, side 23 ff.
  - Fx kryptering ved europæisk mellemled -> vigtigt at forstår det tekniske setup

Djævlen ligger ofte i detaljen

- Kompliceret at vurdere om tilbudt teknisk foranstaltning reelt er effektiv
- IT-kyndige må involveres
- Se eksempel 6-8 i Datatilsynets vejledning om cloud
  - Eksempel 6 -> Kryptering in transit og at rest, men ikke in motion…
  - Eksempel 7 -> Geoblocking af IP adresser -> ej kontrol over underliggende infrastruktur
  - Eksempel 8 -> Europæisk mellemled -> Doctolib

EDPB gennemgår en række scenarier

- Afsnit 93-97 -> scenarier hvor tekniske foranstaltninger ikke vil være effektive i forhold til at sikre "essentially equivalence"

Eksempler:

1. Overførsel til cloud leverandør eller andre databehandlere, der har brug for adgang til data i klartekst

2. Fjernadgang til oplysninger til forretningsformål

-> Fx overførsler inden for en koncern

=> Fælles at adgang til oplysninger i klartekst

Utilsigtede tredjelandsoverførsler

De "utilsigtede" tredjelandsoverførsler

Hvad taler vi om?

- En databehandler beliggende i EU/EØS, der ikke har fået en instruks om at overføre personoplysninger til 3L, bliver – qua virksomhedens koncernstruktur – pålagt af en myndighed i et 3L at udlevere oplysninger til myndigheder i 3L
  - Pålæg om udlevering med ekstraterritorial virkning
  - Utilsigtet (og uønsket) 3L overførsel set fra kundens vinkel (se slide 22 modsætningsvist)
  - En instruks herom ville være i strid med GDPR kap. II og V
    - Manglende behandlingsgrundlag i kap. II
    - Manglende grundlag for 3L-overførsel

- "US Cloud Act"
  - Nok også relevant under FISA 702
  - Formentlig relevant for de fleste 3L

De "utilsigtede" tredjelandsoverførsler

- Når overførsel er utilsigtet for dataansvarlig -> GDPR kap. II og V er ikke udløst for DA (men for DB!)

- GDPR art. 28.1. og 32 skal overholdes
  - Dataansvarlig skal inden brug af databehandler anmode databehandler om at tilkendegive,
    - hvorvidt denne (eller nogen underdatabehandler) er underlagt lovgivning i et 3L
    - som - til trods af en instruks om det modsatte – kan pålægge databehandler at udlevere oplysninger til myndigheder i 3L

De "utilsigtede" tredjelandsoverførsler

Løsning?

- Pre-screening af databehandler, jf. art. 28.1
- Tilstrækkeligt sikkerhedsniveau, jf. art. 32, på baggrund af risikovurdering

Risiko: Sandsynlighed x Konsekvens

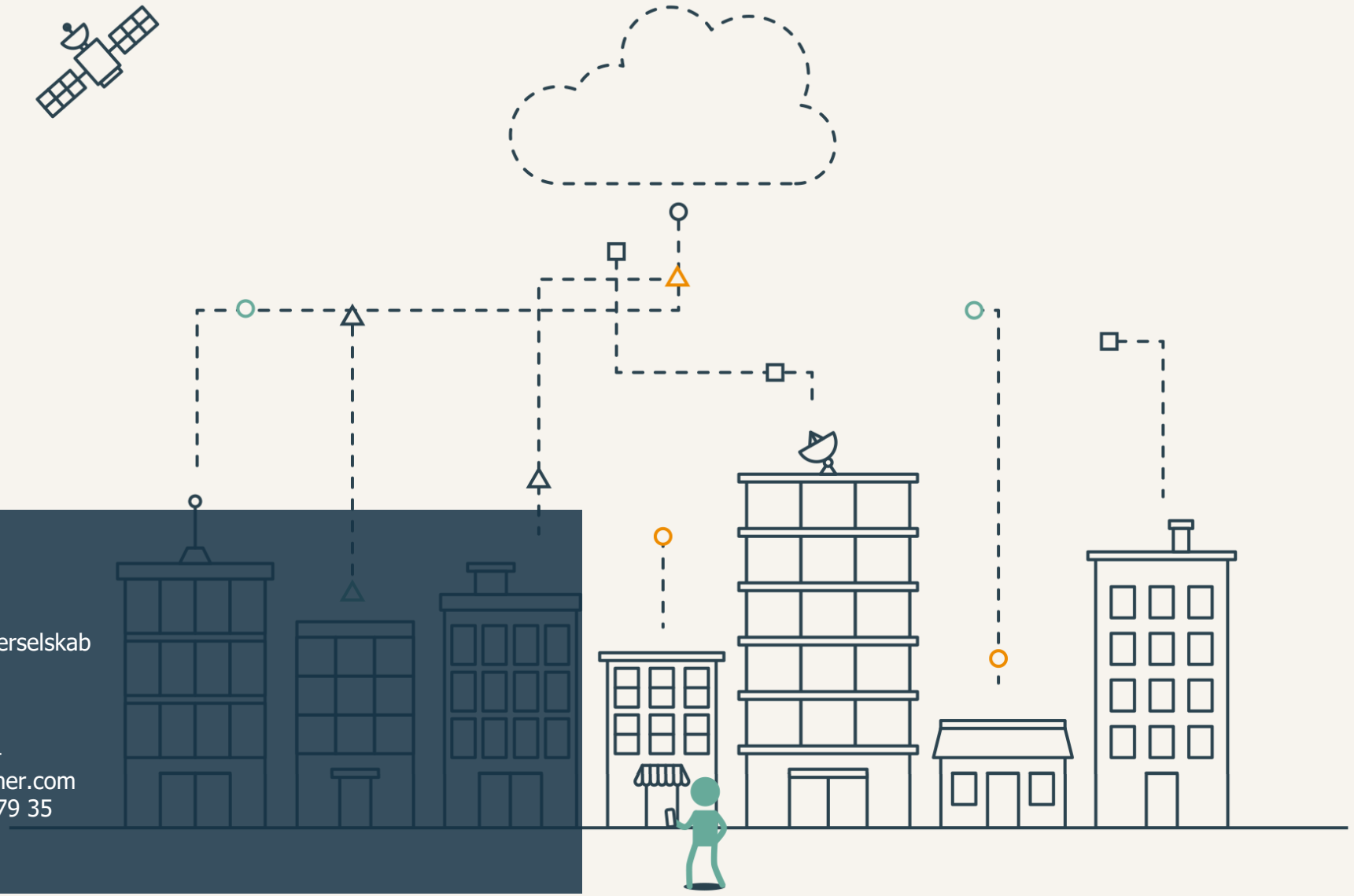
Trussel? F.eks. CLOUD Act anmodning fra amerikanske retshåndhævende myndigheder

- Sandsynlighed? Se bl.a. på statistik over antallet af anmodninger, som databehandleren har modtaget over en årrække, hvilke type(r) af oplysninger, der skal behandles mv.
- Konsekvens? Typer af oplysninger; krænkelse af de registrerede, hvis oplysninger havner hos 3L myndigheder?

Konklusion?

- Hvis risikoen er tilstrækkeligt lav, så kan behandlingen iværksættes – ellers ikke
- Hvis senere kendskab til utilsigtet 3L overførsel – revurdere art. 32 og art. 28.1

Spørgsmål?



Plesner

Plesner Advokatpartnerselskab
Amerika Plads 37
2100 København Ø
Tlf.: +45 33 12 11 33
Fax: +45 33 12 00 14
E-mail: plesner@plesner.com
CVR-nummer: 38 47 79 35

PLESNER