Brug af cloudservices

Gå-hjem møde v/ it-sikkerhedsspecialist
Allan Frank og souschef Makar Juhl Holst

DATATILSYNET

Program

- Datatilsynets vejledning: Hvem og hvorfor?
- Kend dine services
- Kend dine leverandører
- Tilsyn med cloudleverandøren og eventuelle underleverandører
- Tredjelandsoverførsler
- Cloud og USA
- ”Tilsigtede” v. ”utilsigtede” tredjelandsoverførsler

Datatilsynets vejledning: Hvem og hvorfor?

Hvem?

- Dataansvarlige organisationer
- Cloudleverandører
- ”Mellemled”

Hvorfor?

- Vejledning
- Italesætte ukendte størrelser
- Forandring i markedet

Kort om cloud

On premise	IaaS	PaaS	SaaS
Data	Data	Data	Data
Applikationer	Applikationer	Applikationer	Applikationer
Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S
Virtualisering	Virtualisering	Virtualisering	Virtualisering
Server	Server	Server	Server
Lager	Lager	Lager	Lager
Netværk	Netværk	Netværk	Netværk

For uddybning se Datatilsynets cloudvejledning og Digitaliseringsstyrelsens vejledning om anvendelse af cloud

Kend dine services

Afklar faktum – Kortlæg dine datastrømme

- Hvad? Hvordan? Hvorfor?

Risikovurdering vedrørende databeskyttelse

- Lighedstræk med gennemførelse af konsekvensanalyse

Risikovurdering vedrørende behandlingssikkerhed

- Gennemfør risikovurdering (om nødvendigt)
- Afdæk eksisterende sikkerhedsniveau
- Sammenhold med det niveau, du finder nødvendigt

Kend dine leverandører

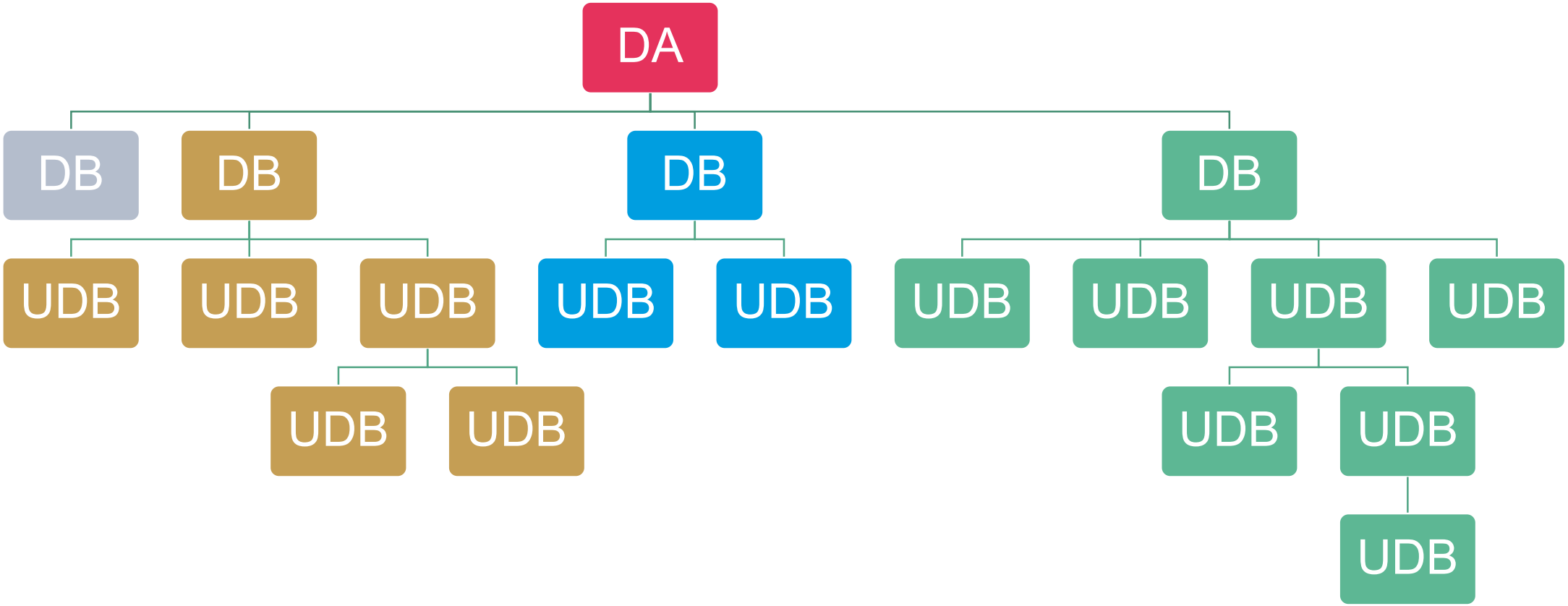
Screening af (cloudleverandører)

- *”Kan leverandøren overholde GDPR ved behandling af persondata, som jeg har ansvaret for?”*
- Udg.pkt.: Databehandleraftalen – se også Datatilsynets standardaftale

OBS!

- Instruks og leverandørens behandling til egne formål
- Brug af underdatabehandlere
  - Screening af underdatabehandlere
  - Udskiftning af underdatabehandlere
- Back-to-back vilkår

Kend dine leverandører



DATATILSYNET

Dokumentation

Vores forventninger

- Beskrivelse af behandlingsaktiviteten, herunder behandlingsgrundlag – Artikel 5-22
  - Risikovurdering vedrørende databeskyttelse – Artikel 24 og 25
- Screening af (cloud)leverandøren – Artikel 28, stk. 1
- Databehandleraftale – Artikel 28, stk. 3
  - Back-to-back vilkår med underdatabehandlere – Artikel 28, stk. 4
- Risikovurdering vedrørende behandlingssikkerhed – Artikel 32, stk. 1
- Beskrivelse eller oversigt over etablerede behandlingssikkerhedsniveau – Artikel 32, stk. 1

Tilsyn med cloudleverandøren og evt. underleverandører

Hvad skal påses?

- Overholdelse af databehandleraftalen

Intensitet og hyppighed

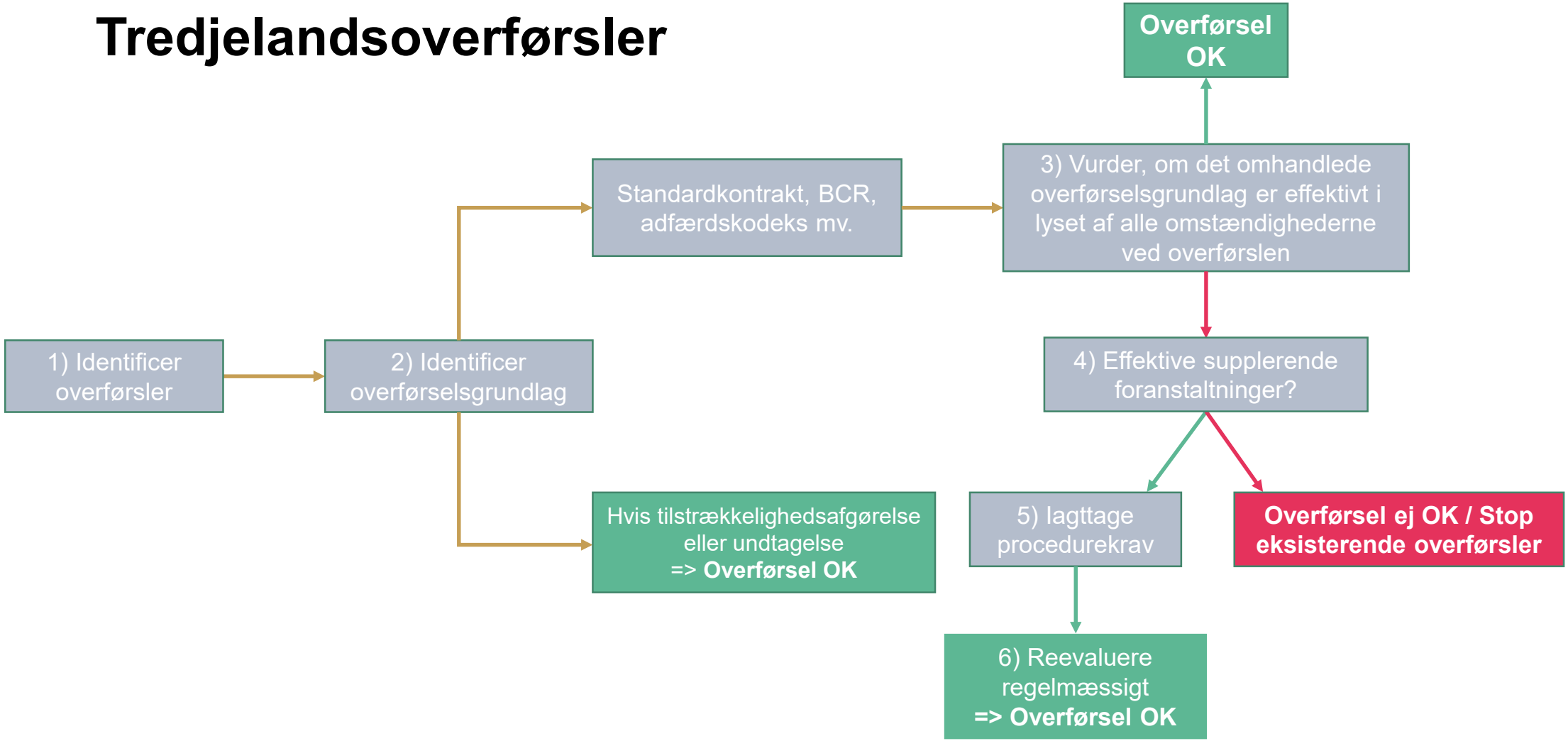
- Udg.pkt.: Risici for de registreredes rettigheder
  - Typen og mængden af persondata, behandlingsaktivitetens karakter
  - Udsving i drift, sikkerhedsbrud

Særligt for cloud

- Revisionserklæringer kan være nok
- OBS! Omfang og metode
- Sikre ret til at kræve andet omfang og/eller metode

DATATILSYNET

Tredjelandsoverførsler



DATATILSYNET

Cloud og USA

- **FISA 702** og **E.O. 12 333** danner retsgrundlag for en række overvågningsprogrammer, som årligt (gen)certificeres ved en domstol
- **CJEU i Schrems II**: FISA 702 og E.O. 12 333, sammenholdt med PPD-28, opfylder ej EU-retten
- ”Electronic communications service providers” – cloud – som derfor ofte er omfattet af ”problematisk lovgivning”
- Betingelser i lovgivningen læst i sammenhæng med retshåndhævende myndigheders målretningsprocedurer, herunder U.S. Person (”USP”) vs. non-USP og ”reasonably belived to be located outside the United States”

Hvad så?

1) Vurdere om lovgivningen finder anvendelse på de relevante overførsler **eller**
2) Træffe supplerende foranstaltninger

DATATILSYNET

Cloud og USA

Finder lovgivningen anvendelse på relevante overførsler i praksis?

- ”foreign intelligence purpose”
  - ”med rimelighed skal vurdere – baseret på alle omstændigheder – at målet forventes at besidde, modtage og/eller sandsynligvis vil kommunikere udenlandsk efterretningsinformation vedrørende en fremmed magt eller fremmed territorium”
  - Bred afgrænsning, som man almindeligvis ikke har nødvendige forudsætninger for at vurdere nærmere
- Brug af selectors
  - Udtømmende oversigt?

- Dataansvarlig og databehandler skal dokumentere sin vurdering af, at lovgivningen ikke finder anvendelse
- Vurdering skal være baseret på objektiv, troværdig og tilgængelig information

Cloud og USA

Supplerende foranstaltninger

- **Organisatoriske**
  - fx procedurer for håndtering af anmodninger fra offentlige myndigheder, uddannelse af medarbejdere mv.
- **Kontraktuelle**
  - fx forpligtelser om at anfægte anmodninger fra myndigheder, forpligtelser om transparens mv.
- **Tekniske**
  - fx kryptering, multi-party computation mv.

Læs mere: EDPB's anbefalinger om supplerende foranstaltninger

”Tilsigtede” v. ”utilsigtede” tredjelandsoverførsler

- Ren ”EU-leverancemodel” – også med hensyn til support, infrastruktur mv.
- Anmodninger fra tredjelande, hvor moderselskab er etableret, fx USA

Hvad skal du gøre?

1) Garantier for, at leverandøren vil overholde GDPR og europæisk ret
2) Sikre nødvendige behandlingssikkerhed, dvs. vurdere risiko for, at databehandleren handler i strid med sine løfter => Risikovurdering og sikkerhedsforanstaltninger
3) Tilsyn med databehandleren

Læs mere: EDPB & EDPS's svar til LIBE komiteen om US CLOUD Act og Datatilsynets svar til KOMBIT

Tak for i dag

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

DATATILSYNET