BECH-BRUUN

Persondataseminar:

Den nye dataforordning – en dag med spørgsmål og svar for behandlere

Odense, den 28. februar 2018

BECH-BRUUN

Program

Kl. 9.00:	Velkomst – mål med dagens program
Kl. 9.10:	Introduktion til persondataretten
Kl. 10.30:	Pause
Kl. 10.50:	Databehandlere og dataansvarlige
Kl. 11.15:	Den registreredes rettigheder og (nationale dataoverførsler)
Kl. 12.00:	Frokost
Kl. 13.00:	HR og persondata
Kl. 14.00:	Praktisk compliance og ”accountability”
Kl. 14.30:	Pause
Kl. 14.50:	Praktisk compliance og ”accountability” (fortsat)
Kl. 15.30:	Compliance nu og fremover
Kl. 16.00:	Tak for i dag

BECH-BRUUN

Mål med dagens program – eksempler på fremsendte spørgsmål der skal besvares…

Accountability – hvordan skal det fortolkes?

Hvad indebærer retten til at blive glemt?

Må vi bruge samme hardware privat og arbejdsmæssig?

Er e-mail-adressen en personfølsom oplysning?

Hvad er personfølsomme data? (særlige-/almindelige personoplysninger).

Hvad vil det sige at være dataansvarlig?

Hvad vilde sige at være databehandler?

Hvad skal vi være særlig opmærksom på ift journalisering - opbevaring af deres data - de noter vi laver til hver session. Er der nogle ting vi skal ændre eller være særlig opmærksomme på?

Er der noget i den nye forordning ang. live konsultationer over Skype eller andre lignende programmer?

Forudsætning for dagens tema

Privatlivsfred (privacy) = retten til at blive ladt i fred (the right to be left alone): Oxford 1870

Privatlivs beskyttelse (data protection) = det vi gør, når vi 'invaderer' privatlivsfreden

Status på forordningen og tidsplan

- Forordning 679/2016
- Justitsministeriets betænkning nr. 1565
- Lovforslag til databeskyttelseslov fremsat i Folketinget
- Vejledninger fra Datatilsynet

Vejledninger – praktisk anvendelige

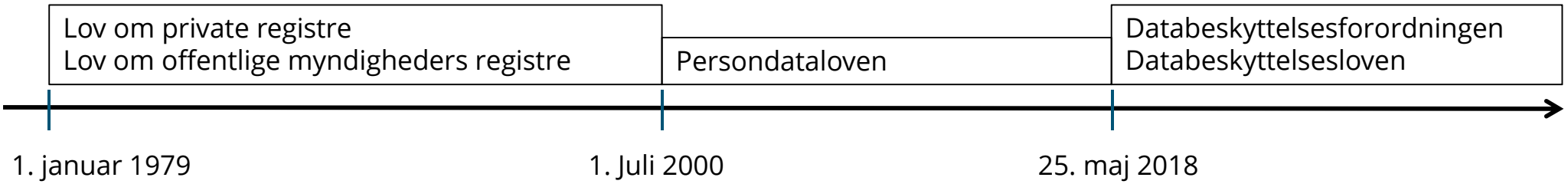
Emne	Offentliggørelse
Generel informationspjece om forordningen	September 2017
Databeskyttelsesrådgiver (DPO)	September 2017
Overførsel af personoplysninger til tredjelande	September 2017
Dataansvarlige og databehandlere	Oktober 2017
Samtykke	Oktober 2017
Fortegnelse	November 2017
Adfærdskodekser og certificeringsordninger	December 2017
Behandlingssikkerhed	December 2017
Databeskyttelse gennem design og standardindstillinger	December 2017
Konsekvensanalyse (DPIA)	December 2017
Cloud computing	December 2017
Håndtering af brud på persondatasikkerheden	Januar 2018
Registreredes rettigheder	Januar 2018

BECH-BRUUN

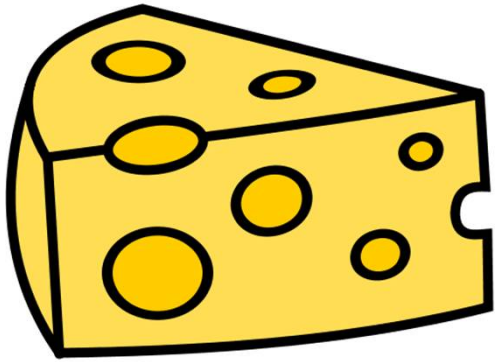
Introduktion til persondataretten

BECH-BRUUN

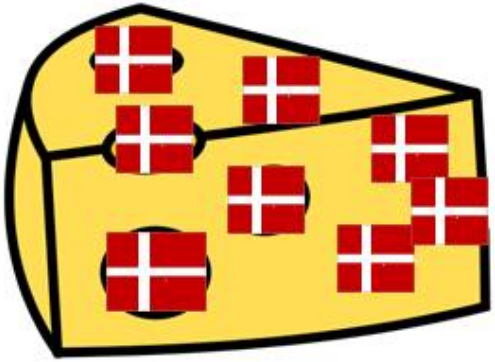
Kort historisk overblik over persondataretten



Databeskyttelsesforordningen



Databeskyttelsesforordningen + Databeskyttelsesloven



Databeskyttelsesloven (udkast)

- **Videreførelse af en lang række regler, herunder:**
  - Behandling af oplysninger om strafbare forhold (§ 8)
  - Behandling af oplysninger om personnumre (§ 10)
  - Aldersgrænsen for samtykket fra børn og unge til brug af informationssamfundstjenester (fx hjemmesider og apps mv.) sættes til 13 år
- For private dataansvarlige skal den dataansvarliges oplysningspligt og den registreredes indsigtsret ikke gælde, "*hvis den **registreredes interesse i oplysningerne findes at burde vige for afgørende hensyn til private interesser,** herunder hensynet til den pågældende selv*"
- **Bøder til offentlige myndigheder** på op til fire procent af driftsbevillingen maksimalt 16 millioner kroner
- Oplysninger om personer, **som har været døde i 10 år**, er ikke længere personoplysninger
- **Anmeldelsesordningen** for kreditoplysningsbureauer og advarselsregistre videreføres
- **Krigsreglen** modificeres og videreføres
- Offentlige myndigheders mulighed for at behandle oplysninger til uforenelige formål

BECH-BRUUN

Definitioner

Definitioner

- Persondataloven indeholder en række væsentlige definitioner (§ 3):
  - Personoplysninger
  - Behandling
  - Den registrerede
  - Dataansvarlig
  - Databehandler
  - Tredjemand
  - Samtykke

- Forordningen tilføjer en række yderligere væsentlige definitioner (artikel 4), bl.a.
  - Helbredsoplysninger
  - Profilering
  - Pseudonymisering
  - Biometriske data

Personoplysninger

- **Definition**: Oplysninger om identificerede eller identificerbare fysiske personer

- <u>"Fysisk person":</u>
  - Oplysninger om fysiske personer
  - Oplysninger om enkeltmandsvirksomheder
  - Oplysninger om mindre I/S'er (mellem fysiske personer)
  - Oplysninger om at en person er aktionær/anpartshaver, bestrider en bestemt stilling, er kontaktperson i et selskab
  - Også oplysninger om bipersoner
  - Ikke juridiske personer

- <u>Forordningen:</u>
  - Oplysninger om afdøde personer (medlemslande beslutter om omfattet)
  - Juridiske persons navn, form og kontaktoplysninger er ikke omfattet

Personoplysninger

- Personoplysninger
  - Alle oplysninger uanset form, hvis det er praktisk muligt at henføre oplysningerne til en bestemt fysisk person
  - Også pseudonyme oplysninger
    - **Definition**: behandling af personoplysninger på en sådan måde, at oplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger, så længe sådanne supplerende oplysninger opbevares separat og er underlagt tekniske og organisatoriske foranstaltninger for at sikre, at henførsel til en identificeret eller identificerbar person ikke kan forekomme
  - Ikke **anonyme** oplysninger (strenge krav – ingen må kunne føre oplysninger tilbage)
  - Ikke **aggregerede** oplysninger (strenge krav – minimumsinterval)
- Forordningen
  - Helbredsoplysninger er personoplysninger, der vedrører en persons fysiske eller mentale helbred, herunder levering af sundhedsydelser, og som giver information om vedkommendes helbredstilstand

BECH-BRUUN

Hvad er personoplysninger?

Anonyme oplysninger ÷

Pseudonyme oplysninger ✓

Cpr-nr.

Køn

Navn

Race

Adresse

E-mail-adresse

Seksuel overbevisning

Foto

Fødselsdato

Kreditkortnummer

Adgangskontrol

Helbredsoplysninger

Nummerplade

Genetisk information

Interesser

Familiemæssige oplysninger

MedarbejderID

Politisk overbevisning

Væsentlige sociale problemer

Uddannelse (karakterer)

Personlighedstest

Telefonnummer

Religion

Personlige produktionstal

IP-adresse

Elektroniske spor

Videoovervågning

Pasnr.

GPS-oplysninger

Logning i IT-systemer

Initialer/Loginnavn

Fagforeningsmæssige tilhørsforhold

Biometriske oplysninger

Straffeattest

Stilling

Størrelse på tøj og sko

Rejseoplysninger

MAC-adresse

Løn

Oplysningskategorier

	Persondataloven		Persondataforordningen
Almindelige oplysninger	Fx • Navn • Adresse • E-mail		Også • Oplysninger om strafbare forhold* • Sociale problemer • Andre rent private forhold end følsomme oplysninger
Semi-følsomme oplysninger	• Oplysninger om strafbare forhold • Sociale problemer • Andre rent private forhold end følsomme oplysninger		
Følsomme oplysninger	• Racemæssig eller etnisk baggrund • Politisk, religiøs eller filosofisk overbevisning • Fagforeningsmæssige tilhørsforhold • Oplysninger om helbredsmæssige eller seksuelle forhold		• Racemæssig eller etnisk baggrund • Politisk, religiøs eller filosofisk overbevisning • Fagforeningsmæssige tilhørsforhold • Behandling af genetiske data eller biometriske data med henblik på unik identifikation • Oplysninger om helbredsmæssige eller seksuelle forhold
Cpr-nr.	• Offentlige myndigheder: Mhp. entydig identifikation/journalnummer • Private virksomheder: Lovbestemmelse/samtykke • Aldrig offentliggørelse uden samtykke		• Medlemsstater kan fastsætte specielle betingelser, dog krav om tilstrækkelige sikkerhedsforanstaltninger

Behandling

Definition: Enhver håndtering af oplysninger med eller uden brug af automatiseret databehandling

- Eksempler
  - Indsamling, registrering, systematisering, brug, opbevaring, tilpasning, ændring, selektion, søgning, offentliggørelse på internettet mv., samkøring, videregivelse, overladelse, overførsel, blokering, begrænsning, sletning, tilintetgørelse, intern anvendelse, anonymisering

ALT ER BEHANDLING

Personkredsen

Personkredsen udgøres af følgende:

- Registrerede (datasubjekter):
  - Den, de pågældende personoplysninger omhandler
- Dataansvarlig:
  - Den, der bestemmer, til hvilket formål og med hvilke hjælpemidler, behandlingen foretages
- Databehandler:
  - Den, der behandler oplysninger på den dataansvarliges vegne
- Tredjemand:
  - Andre end de ovenstående

Forordningen (artikel 26):

- Fælles dataansvarlige → hvis to eller flere dataansvarlige i fællesskab fastlægger formålene med og midlerne til behandling af personoplysninger

Samtykke

En viljestilkendegivelse, der skal være frivillig, specifik, og informeret:

- **Frivillig**: Uden tvang eller andet pres, reelt og frit valg, kan afvise/tilbagetrække samtykket uden at det er til skade for den pågældende
  - Medarbejdersamtykke
- **Specifik**: Konkret samtykke til en konkret behandling (så detaljeret beskrevet som muligt)
- **Informeret**: Tilstrækkelig beskrivelse af hvad der gives samtykke til

- Samtykke i erklæring med andre forhold:
  - Skal klart kunne skelnes fra andre forhold
  - Letforståelig og lettilgængelig form i et enkelt og klart sprog
- Ugyldigt samtykke medfører, at pågældende del af erklæring ikke er bindende
- Den registreret skal informeres om mulighed for at trække samtykke tilbage inden afgivelse – skal være lige så let at trække tilbage som af afgive
- Er samtykket anvendt til behandling af yderligere oplysninger, som ikke er nødvendige for opfyldelse af kontrakt?
- Børns (indtil 13 år) samtykke i forbindelse med informationssamfundstjenester – skal gives af forældremyndighedsindehaver (artikel 8)

Profilering

- **Definition**: enhver form for automatisk behandling af personoplysninger, der består i at anvende de pågældende oplysninger til at evaluere bestemte personlige forhold vedrørende en fysisk person, navnlig for at analysere eller forudsige forhold vedrørende den fysiske persons arbejdsindsats, økonomiske situation, helbred, personlige præferencer, interesser, pålidelighed, adfærd, opholdssted eller bevægelser

- Eksempler:
  - Kreditvurdering
  - Kundeprofiler
  - Personlighedsanalyser

Databeskyttelsesforordningens territoriale anvendelsesområde

Dataansvarlig/databehandler etableret i EU

- Persondataforordningen finder anvendelse på behandling af personoplysninger, som foretages for en dataansvarlig/databehandler etableret i EU, uanset om behandlingen finder sted i EU eller ej

Dataansvarlig/databehandler etableret uden for EU

- Hvor den dataansvarlige/databehandleren er etableret uden for EU, finder persondataforordningen alene anvendelse på behandling af personoplysninger om registrerede bosiddende i EU, hvis behandlingsaktiviteterne vedrører:
  - Udbud af varer/tjenesteydelser til den registrerede bosiddende i EU
  - Overvågning af den registreredes adfærd, hvis adfærden finder sted i EU

Databeskyttelsesforordningens territoriale anvendelsesområde – Ændringer

- I store træk videreføres gældende ret
- Dog kan fremhæves følgende ændringer:

Udvidelse →

PDL/PDD: Regulerer alene dataansvarliges behandling af personoplysninger

GDPR: Regulerer også databehandlerens behandling

Indskrænkning →

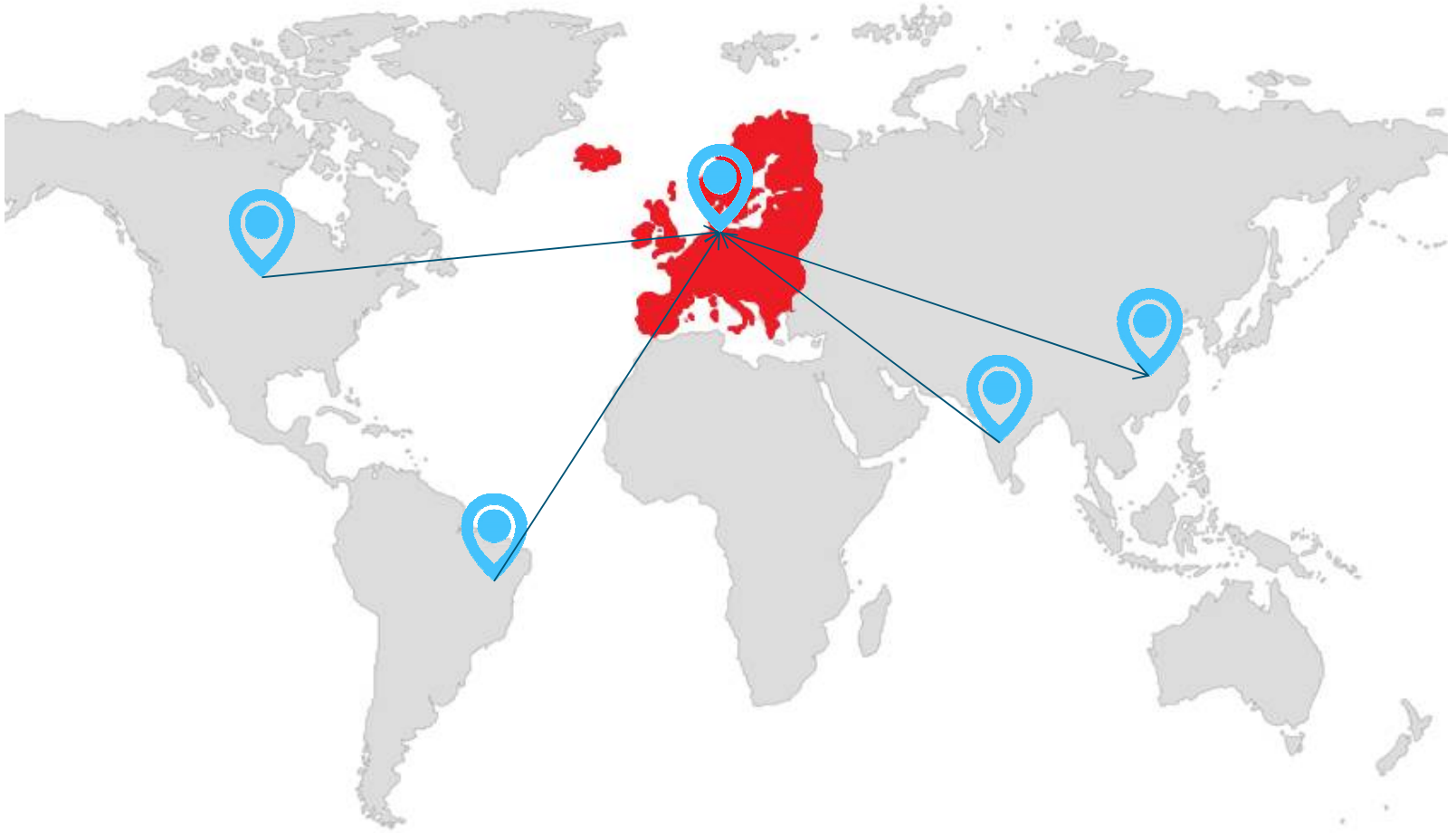
PDL/PDD: Finder anvendelse på dataansvarlige etableret uden for EU, hvor:

- behandling af oplysninger sker under benyttelse af hjælpemidler, der befinder sig i Danmark eller
- indsamling af oplysninger i Danmark sker med henblik på behandling uden for EU

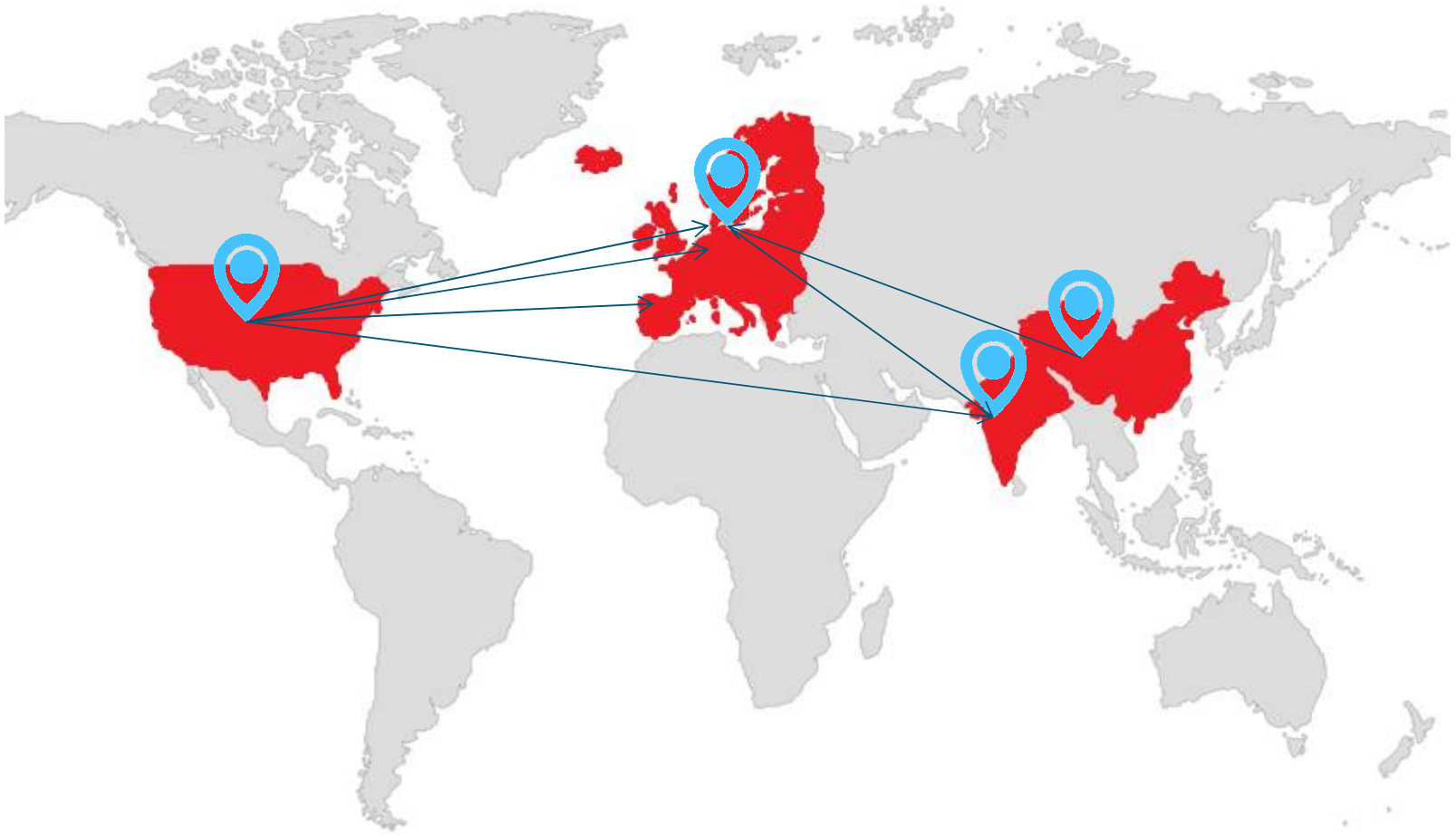
GDPR: Finder *alene* anvendelse på dataansvarlige/databehandlere etableret uden for EU, hvis behandlingsaktiviteter vedrører:

- udbud af varer/tjenesteydelser til den registrerede bosiddende i EU *eller*
- overvågning af den registreredes adfærd, hvis adfærden finder sted i EU

24. maj 2018



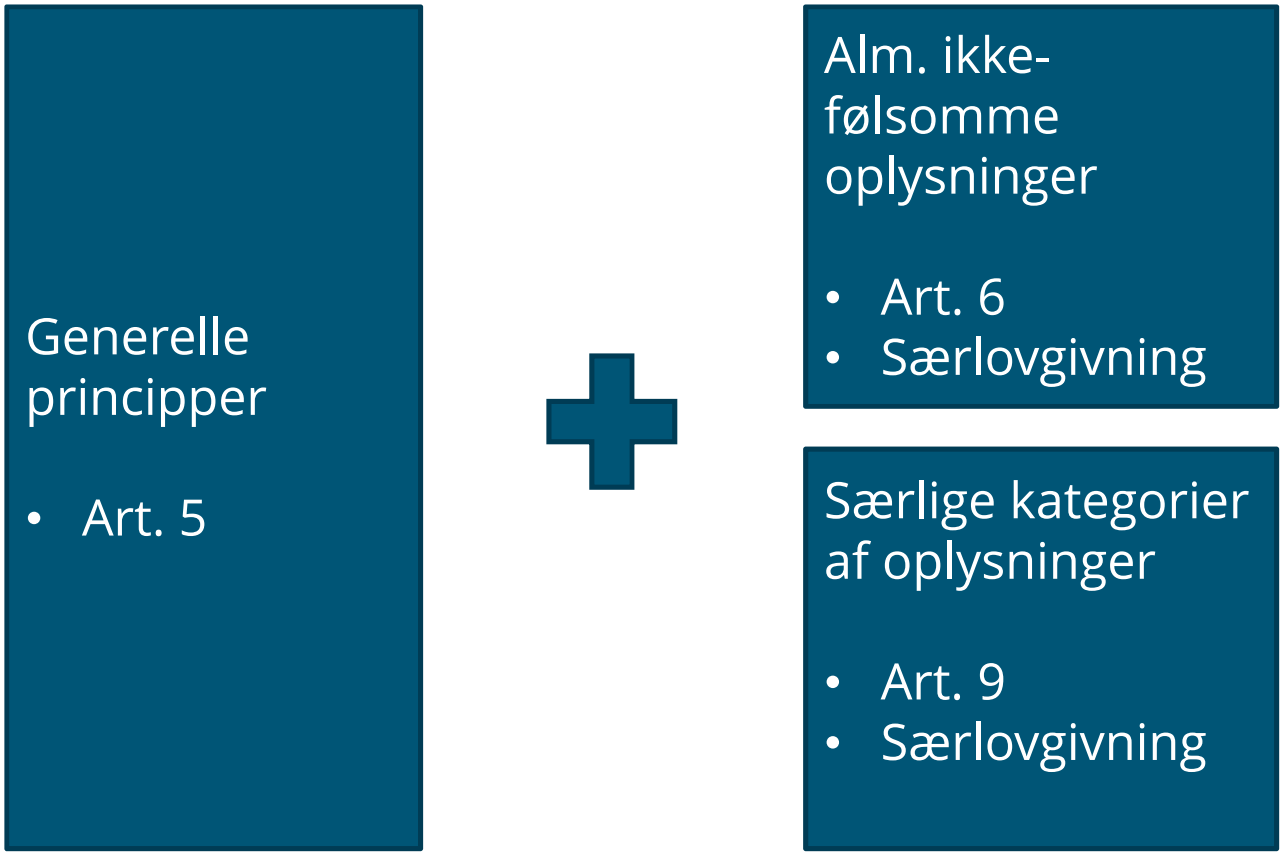
25. maj 2018



BECH-BRUUN

Grundlæggende principper og retligt grundlag

Betingelser for at behandle personoplysninger



Grundlæggende behandlingsprincipper (artikel 5)

- **Princippet om lovlighed, rimelighed og gennemsigtighed**: Personoplysninger skal behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede

- **Princippet om formålsbegrænsning**: Personoplysninger skal indsamles til udtrykkeligt angivne og legtime formål. Viderebehandling må ikke være uforenelig med det oprindelige formål.

  - (Viderebehandling til arkivering i samfundets interesse eller til videnskabelige og historiske forskningsformål eller statistiske formål i overensstemmelse med artikel 89, stk. 1, er ikke uforeneligt med det oprindelige formål)

- **Princippet om dataminimering**: Personoplysninger skal være relevante, tilstrækkelige og begrænset til, hvad der er nødvendigt i forhold til behandlingsformålet

Grundlæggende behandlingsprincipper

- **Princippet om rigtighed**: Personoplysninger skal være rigtige og om nødvendigt ajourførte. Der skal tages ethvert rimeligt skridt for at sikre, at urigtige personoplysninger straks slettes eller berigtiges (under hensyn til behandlingsformål)

- **Princippet om opbevaringsbegrænsning**: Personoplysninger skal opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til behandlingsformålet

- **Princippet om integritet og fortrolighed**: Personoplysninger skal behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende oplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger

- **Princippet om ansvarlighed**: Den dataansvarlige er ansvarlig for og være i stand til at påvise, at de grundlæggende principper overholdes

    - Præcisering af, at det er den dataansvarlige, som skal kunne **påvise** – i modsætning til databeskyttelsesdirektivets krav om, at den dataansvarlige skal **sikre** – at behandlingsprincipperne skal overholdes.

Behandling af almindelige oplysninger (artikel 6)

- Behandling af almindelige personoplysninger kun lovligt, hvis mindst ét af nedenstående retlige grundlag (stk. 1):

a) Registrerede har **givet samtykke** til behandling til ét eller flere specifikke formål

Behandling nødvendig:

b) For at **opfylde aftale** eller forud for indgåelse af aftale (eller på registreredes anmodning forud herfor)

c) For at **overholde retlig forpligtelse**, som gælder for den dataansvarlige

d) For at beskytte den registreredes eller anden fysisk persons **vitale interesser**

e) For at udføre en opgave i **samfundets interesse** eller i forbindelse med offentlig **myndighedsudøvelse**, som den dataansvarlige har fået overdraget

f) Af hensyn til dataansvarliges (eller tredjemands) **legitime interesse**, med mindre registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse af personoplysninger, går forud herfor, navnlig hvis registrerede er et barn.
Gælder ikke for offentlige myndigheders behandling som led i myndighedsopgaver

Behandling af følsomme oplysninger (artikel 9)

- Særlige kategorier af personoplysninger
- Personoplysninger om racemæssig eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning og fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data for entydigt at identificere en person eller oplysninger om helbredsforhold eller seksuelle forhold og seksuel orientering
- Udg. pkt.: Behandling forbudt
- Forbud gælder ikke, hvis
  - Den registrerede har givet sit udtrykkelige **samtykke**
  - Nødvendig behandling på bl.a. det **arbejdsretlige område med hjemmel i lovgivning**
  - Nødvendig behandling for at beskytte registreredes (eller anden persons) **vitale interesser** – ikke selv i stand til at samtykke
  - **Politiske, religiøse, faglige stiftelse/sammenslutningers** behandling af oplysninger med medlemmer – ingen videregivelse uden samtykke
  - Oplysningerne er tydeligvis **offentliggjort af den registrerede**
  - Nødvendig behandling for at **et retskrav kan fastlægges**, gøres gældende eller forsvares eller når domstol handler i egenskab af domstol

Behandling af følsomme oplysninger (artikel 9)

- Nødvendig behandling af hensyn til væsentlige samfundsinteresser på grundlag af lovgivning
- Nødvendig behandling inden for sundhedsområdet af personer underlagt tavshedspligt
- Nødvendig behandling mhp. arkivering i samfundets interesse, videnskabelige eller historiske forskningsformål eller statistiske formål

> ”Behandling er nødvendig af hensyn til væsentlige samfundsinteresser på grundlag af EU-retten eller medlemsstaternes nationale ret og står i rimeligt forhold til det mål, der forfølges, respekterer det væsentligste indhold af retten til databeskyttelse og sikrer passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser.”

Behandling til andet end oprindelige formål (artikel 6, stk. 4 og § 5, stk. 2)

- Ikke baseret på samtykke eller lovgivning fra EU eller medlemsstat
- Databeskyttelseslovens § 5, stk. 2, gengiver databeskyttelsesdirektivets art. 6(4):

- Dataansvarlige skal afgøre om behandling er foreneligt med oprindeligt formål:
  - eventuel forbindelse mellem det formål, som oplysningerne er indsamlet til, og formålet med den påtænkte viderebehandling
  - den kontekst, hvori personoplysningerne er blevet indsamlet, navnlig med hensyn til forholdet mellem registrerede og dataansvarlige
  - personoplysningernes art, navnlig om særlige kategorier af personoplysninger behandles (følsomme oplysninger eller oplysninger vedrørende straffedomme eller straffelovsovertrædelser)
  - påtænkte viderebehandlings mulige konsekvenser for de registrerede
  - tilstedeværelse af fornødne garantier - kan omfatte kryptering eller pseudonymisering

- Mulighed for at offentlige myndigheder kan viderebehandle oplysninger til andre formål end de oprindelige, selvom formålene ikke er forenelige – delvis fravigelse af oplysningspligten (art. 13(3) og 14(4))

Betingelser for samtykke

- Dataansvarlige kunne bevise, at den registrerede har givet samtykke til behandling af sine personoplysninger
- Enhver **frivillig, specifik, informeret** og utvetydig viljestilkendegivelse fra den registrerede

- Samtykke i erklæring med andre forhold (artikel 7):
  - Skal klart kunne skelnes fra andre forhold
  - Letforståelig og lettilgængelig form
  - Enkelt og klart sprog
- Ugyldigt samtykke medfører, at pågældende del af erklæring ikke er bindende
- Samtykke skal altid kunne trækkes tilbage – være lige så let at trække tilbage som af afgive
- Er samtykket anvendt til behandling af oplysninger, som ikke er nødvendigt for opfyldelse af kontrakt?
- Børns (indtil 13-16 år) samtykke i forbindelse med informationssamfundstjenester – skal gives af forældremyndighedsindehaver

Straffedomme/straffelovsovertrædelser (artikel 10/§ 8)

- Behandling af oplysninger om straffedomme/straffelovsovertrædelser kun foretages
  - Under kontrol af offentlig myndighed
  - Eller hvis behandling er tilladt iht. EU-ret eller national ret
- Ethvert omfattende register over straffedomme kun føres under kontrol af offentlig myndighed

Databeskyttelseslovens § 8:

- Offentlige myndigheder må behandle oplysninger om strafbare forhold når:
  - Det er nødvendigt for varetagelsen af myndighedens opgaver
  - Videregivelse af oplysninger: specifikt opregnede situationer
- Private må behandle oplysninger om strafbare forhold på baggrund når:
  - Den registrerede har givet samtykke
  - Den dataansvarlige har en berettiget interesse, som klart overstiger hensynet til den registrerede
- Videregivelse af oplysninger: Varetagelse af offentlige/private interesser (hensynet til den registrerede), der klart overstiger hensynet til interesser, der begrunder hemmeligholdelse.

BECH-BRUUN

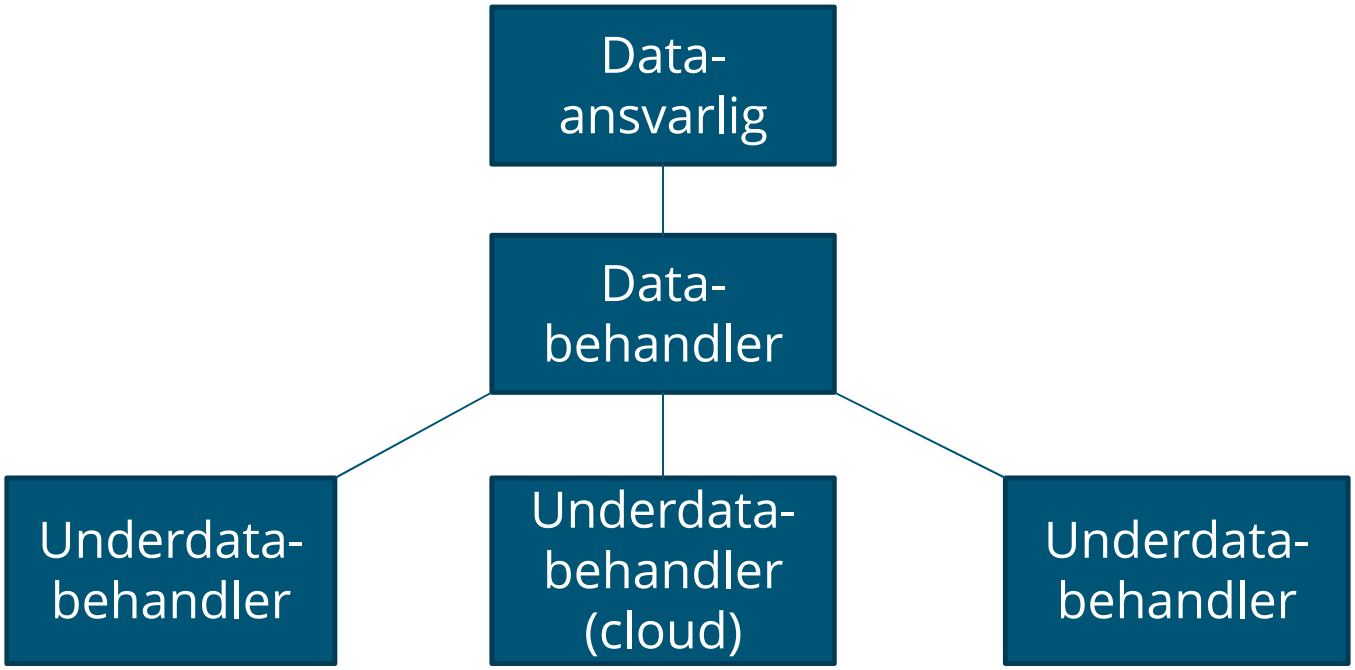
Databehandlere og dataansvarlige

Definitioner

- **Dataansvarlig** (databeskyttelsesforordningens artikel 4, nr. 7):
  - Den fysiske eller juridiske person eller offentlige myndighed, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler, der må foretages behandling af personoplysninger.

- **Databehandler** (databeskyttelsesforordningens artikel 4, nr. 8):
  - Den fysiske eller juridiske person eller offentlige myndighed, der behandler personoplysninger på den dataansvarliges vegne, f.eks.:
    - Udbyder af personlighedstests
    - Lønadministrator
    - Marketingbureau, fx udsendelse af e-mails
    - E-shop leverandør
    - Øvrige systemudbydere/it-leverandører
    - Konsulenter
    - Osv.

Organisationsstruktur



Databehandlerne kan være både eksterne og interne (fx et koncernselskab) og være etableret inden for og uden for EU/EØS

Forholdet mellem parterne

- Lovgivningen fastlægger krav til henholdsvis den dataansvarlige og databehandleren
- Man kan outsource opgaven, men ikke ansvaret!
- Den dataansvarlige og databehandleren kan regulere forpligtelser mellem hinanden

Forpligtelser i henhold til databeskyttelsesforordningen

Den dataansvarlige skal (artikel 28, stk. 1-3):

- Udelukkende benytte databehandlere, der kan stille de fornødne garantier for (**due diligence**)
  - At gennemføre passende tekniske og organisatoriske foranstaltninger med henblik på at overholde databeskyttelsesforordningen
  - At sikre beskyttelse af den registreredes rettigheder
  - Garantier i form af **ekspertise, pålidelighed og ressourcer**

- Løbende sikre, at databehandleren overholder sine forpligtelser (**audit**)

- Indgå en skriftlig **databehandleraftale**
  - Der er bindende for databehandleren
  - Der fastsætter genstanden for og varigheden af behandlingen, behandlingens karakter og formål, typen en af personoplysninger og kategorierne af registrerede samt den dataansvarliges forpligtelser og rettigheder

Databehandleraftalen – indhold

Forordningen stiller endvidere følgende **specifikke krav** til indholdet af databehandleraftalen (artikel 28, stk. 3, litra a-h), så databehandleren:

- Kun må behandle personoplysninger efter dokumenteret instruks fra den dataansvarlig
- Skal sikre, at databehandlerens medarbejdere er underlagt fortrolighed/tavshedspligt
- Iværksætter passende tekniske og organisatoriske sikkerhedsforanstaltninger
- Indhenter godkendelse fra den dataansvarlige ved brug af underdatabehandler
- Bistår den dataansvarlige i forhold til bl.a.
  - At sikre de registreredes rettigheder
  - At sikre overholdelse af kravene til behandlingssikkerhed, notifikation og konsekvensanalyse (DPIA)
- Sletter eller tilbageleverer personoplysninger ved aftalens ophør
- Stiller oplysninger/dokumentation til rådighed for den dataansvarlige og bidrager til revision og inspektioner

Databehandlerens forpligtelser

Databehandleren skal (artikel 28, stk. 2 - 4):

- Indhente den dataansvarliges **godkendelse** ved overladelse af oplysninger til andre/nye under-databehandlere
  - Specifikt samtykke → navngiven underdatabehandler
  - Generelt samtykke → databehandleren skal give underretning inden tilføjelse/erstatning af underdatabehandlere, så den dataansvarlige kan gøre indsigelse
- Indgå skriftlige underdatabehandleraftaler på **back-to-back vilkår**
  - Databehandleren er fortsat ansvarlig over for den dataansvarlige
- Løbende sikre, at underdatabehandlerne opfylder deres forpligtelser (dvs. udfylde den dataansvarliges **audit** forpligtelse)
- Gøre indsigelse, hvis den dataansvarliges instruks er i strid med forordningen eller anden persondataregulering

Databehandleraftalen – indhold

- Øvrige væsentlige forhold:
  - Auditadgang og omfang
  - Hvem afholder udgifterne til fremskaffelse af oplysninger m.v.
  - Notifikationsforpligtelser
  - Fordeling af ansvar – dvs. ud over det, der følger af databeskyttelsesforordningen og de almindelige regler om ansvar i kontrakt
  - Fuldmagt til tredjelandsoverførsler
  - Oversigt over underdatabehandlere
  - Opsigelsesadgang
  - Øvrige krav til databehandleren, f.eks. specifikation af de "organisatoriske og tekniske sikkerhedsforanstaltninger"

- Databehandlere etableret i lande uden for EU/EØS → Kommissionens standardkontrakter

BECH-BRUUN

Den registreredes rettigheder og internationale dataoverførsler

BECH-BRUUN

Den registreredes rettigheder

Den registreredes rettigheder

- Generelt krav om transparens
- Oplysningspligt - hvor oplysninger indsamles fra den registrerede
- Oplysningspligt - hvor oplysninger *ikke* er indhentet hos den registrerede
- Den registreredes ret til indsigt
- Ret til berigtigelse
- Ret til sletning (*"ret til at blive glemt"*)
- Ret til begrænsning af behandling
- Ret til dataportabilitet
- Ret til indsigelse
- Automatiske individuelle afgørelser, herunder profilering

Oplysningspligt - hvor oplysninger indsamles fra den registrerede (artikel 13)

- Oplysningspligt over for den registrerede
- Den registrerede skal oplyses om (minimum):
  - **Dataansvarligs og eventuel repræsentants eller DPO's identitet**
  - **Formålet og retsgrundlaget for behandlingen**
    - Hvis de senere behandles til et andet formål, gives oplysningerne på ny
  - Den dataansvarliges legitime interesse i at behandle oplysninger (hvis hjemmel i art. 6, skt. 1, litra f)
  - **Modtagere eller kategorier af modtagere**
  - Oplysninger om, hvorvidt dataansvarlig agter at videregive oplysninger til tredjeland
  - Registreringens tidsrum eller kriterier til at fastlægge dette
  - **Den registreredes rettigheder** og klagemuligheder, herunder retten til at trække samtykke tilbage
  - Den registreredes eventuelle pligt til at give oplysningerne
  - Om der er tale om automatiske afgørelser – og i givet fald logikken bag og konsekvenserne af sådanne afgørelser
- Gives i forbindelse med indsamlingen – fx ved køb på en hjemmeside
- Kravet gælder ikke, hvis den registrerede er bekendt med oplysningerne

Oplysningspligt – hvor oplysninger ikke er indhentet hos den registrerede (artikel 14)

- Oplysningspligt over for den registrerede
- Oplysninger skal gives til den registrerede inden for rimelig tid og senest en måned efter – eller første gang den registrerede kontaktes med disse, eller senest når der sker videregivelse
- Specielt vedrørende oplysninger, som ikke er indsamlet hos den registrerede (foruden de oplysninger, som også skal gives efter artikel 13):
  - Oplysninger om, hvilken kategori af oplysninger det drejer sig om
  - Oplysninger om, hvorfra oplysningerne stammer

Den registreredes ret til indsigt

- Pligt for den dataansvarlige at oplyse den registrerede om en række oplysninger efter dennes anmodning
- Pligt til at aflevere kopi af de personoplysninger, der behandles – dog med respekt for andres rettigheder og eventuelt mod et rimeligt gebyr
- Hvis den registrerede fremsætter anmoder om indsigt, skal den dataansvarlige oplyse:
  - **Formål**
  - **Kategorier af oplysninger**
  - **Kategorier af modtagere**
  - Registreringens tidsrum eller kriterier til at fastlægge dette
  - Den registreredes rettigheder og klagemuligheder
  - **Tilgængelig information om, hvorfra oplysninger stammer**
  - Tilstedeværelsen af automatisk beslutningstagning og profilering
  - Oplysninger om, hvorvidt dataansvarlig agter at videregive oplysninger til tredjeland

Undtagelser

Artikel 12

- Udøvelse af rettigheder er gratis
  - Medmindre de er åbenbart grundløse eller overdrevne
  - Alternativ kan anmodningen afvises

Betydningen af lovforslag til databeskyttelseslov med undtagelser til rettigheder

- Afgørende hensyn til private interesser i forhold til artikel 13-15
- Hensynet til offentlige interesser i forhold til artikel 13-15
- I samme omfang som offentlighedsloven for offentlige myndigheder i forhold til artikel 15
- Statistisk eller videnskabeligt øjemed i forhold til artikel 15, 16, 18 og 21
- Offentlige myndigheders viderebehandling til et andet formål, jf. artikel 5, stk. 3, i forhold til artikel 13-14

Ret til berigtigelse (artikel 16)

- Nødvendig sondring mellem private og offentlige dataansvarlige, da offentlige dataansvarlige typisk er underlagt modstridende regler – fx offentlighedslovens notatpligt
- Formentlig videreførelse af praksis
- Ny ret til at komplettere ufuldstændige oplysninger
- Oplysningspligt overfor den registrerede

Ret til sletning (”ret til at blive glemt”) (artikel 17)

- + Google-dommen
- Ret til sletning er gammel – ret til at blive glemt er ikke
- Kommende praksis fra Datatilsynet, øvrige medlemslande samt retningslinjer fra Det Europæiske Databeskyttelsesråd (tidligere Art. 29-gruppen)
- Samspil med andre bestemmelser – fx reglerne vedr. samtykke og legitime behandlingsgrunde
- Evt. lovkrav om fortsat opbevaring

Ret til begrænsning af behandling (artikel 18)

- ”Begrænsning” af behandling – ikke sletning af oplysninger
- Den registrerede har ret til begrænsning af behandling af oplysninger, hvis:
  - Rigtigheden af oplysningerne bestrides (indtil rigtigheden er fastslået)
  - Behandlingen er ulovlig
  - Behandlingen ikke længere er nødvendig for behandlingens formål, men er nødvendige for, at retskrav kan fastslås, gøres gældende eller forsvares af den dataansvarlige
  - Den registrerede har gjort indsigelse mod behandlingen i medfør af artikel 21, stk. 1 (indtil behandlingsgrundlagets legitimitet er fastslået).

Ret til dataportabilitet (artikel 20)

- Ny bestemmelse
- Ret til – under visse betingelser – at få udleveret sine oplysninger eller videresendt dem til en ny dataansvarlig
  - Behandling baseret på samtykke eller kontrakt
  - Behandling foretaget automatisk
- Skal være i almindeligt anvendt og maskinlæsbart format
- Betyder nu, at den registrerede ikke længere er fastlåst som brugere af et bestemt medie – fx Facebook.

Ret til indsigelse (artikel 21)

- Ret til at gøre indsigelse overfor dataansvarlig i forhold til behandlinger baseret på artikel 6, stk. 1, litra e og f
- Behandling af personoplysninger med henblik på direkte markedsføring
- Dataansvarlig skal påvise legitime grunde

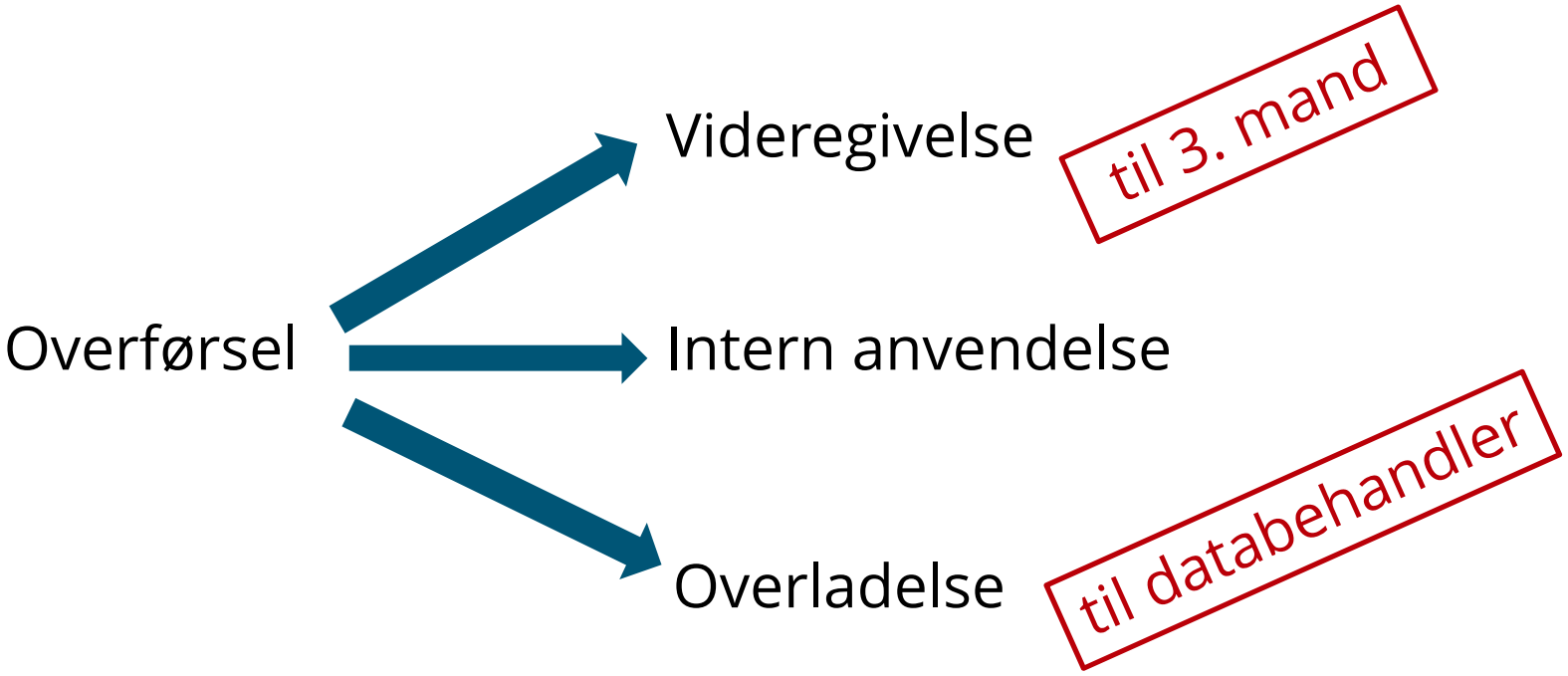
Automatiske individuelle afgørelser, herunder profilering (artikel 22)

- Ikke meget anvendt i DK
- Ret til ikke at være genstand for en afgørelse, som alene er baseret på automatisk behandling – herunder profilering
- Undtagelser:
  - Nødvendig for indgåelse/opfyldelse af kontrakt
  - Hjemmel i EU-ret/national ret
  - Baseret på registreredes udtrykkelige samtykke
- Profilering har ikke tidligere været diskuteret i en særlig grad i dansk databeskyttelse – er traditionelt set betragtet som en "almindelig" behandling af oplysninger

BECH-BRUUN

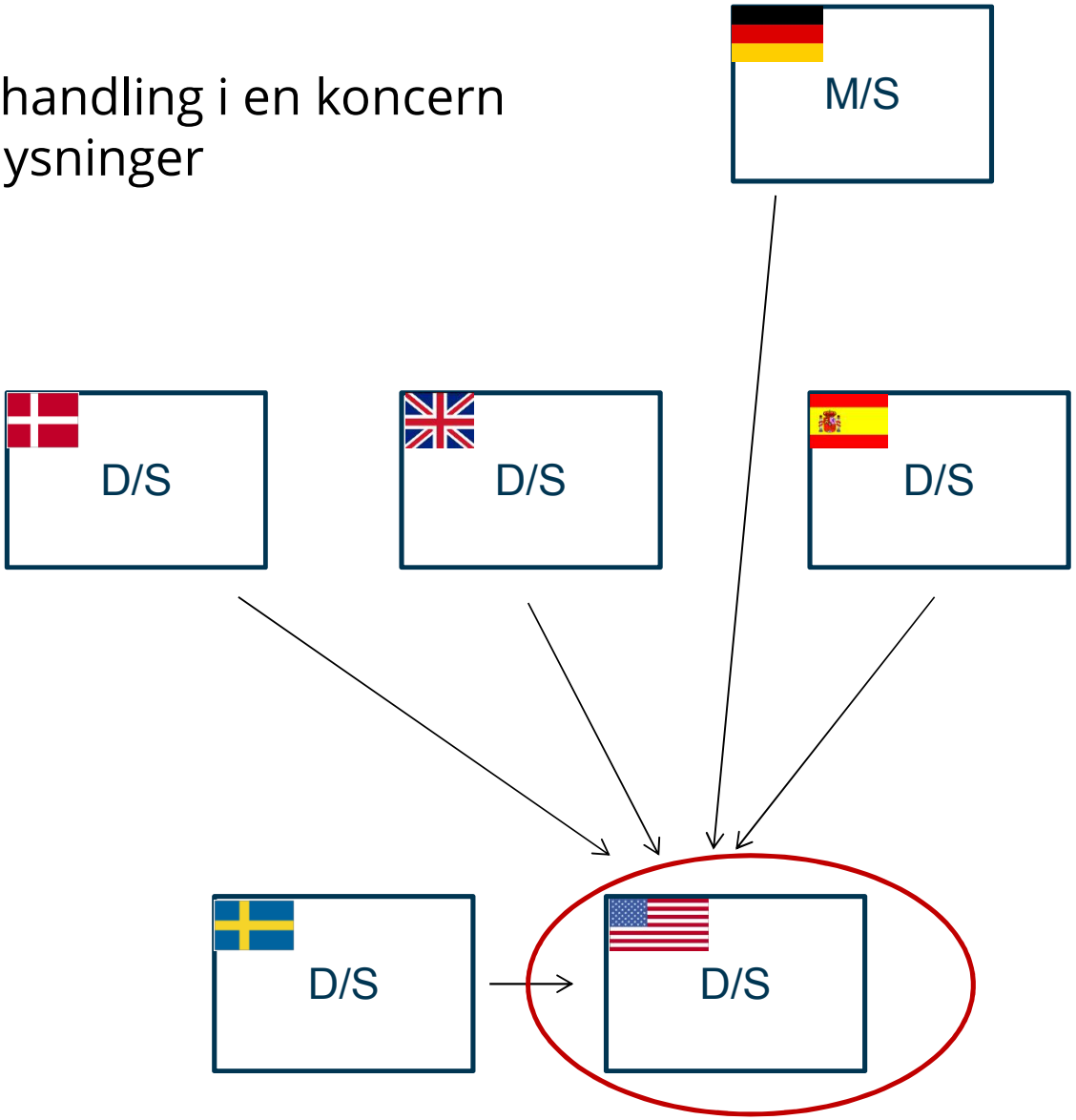
Internationale dataoverførsler

Overførsel

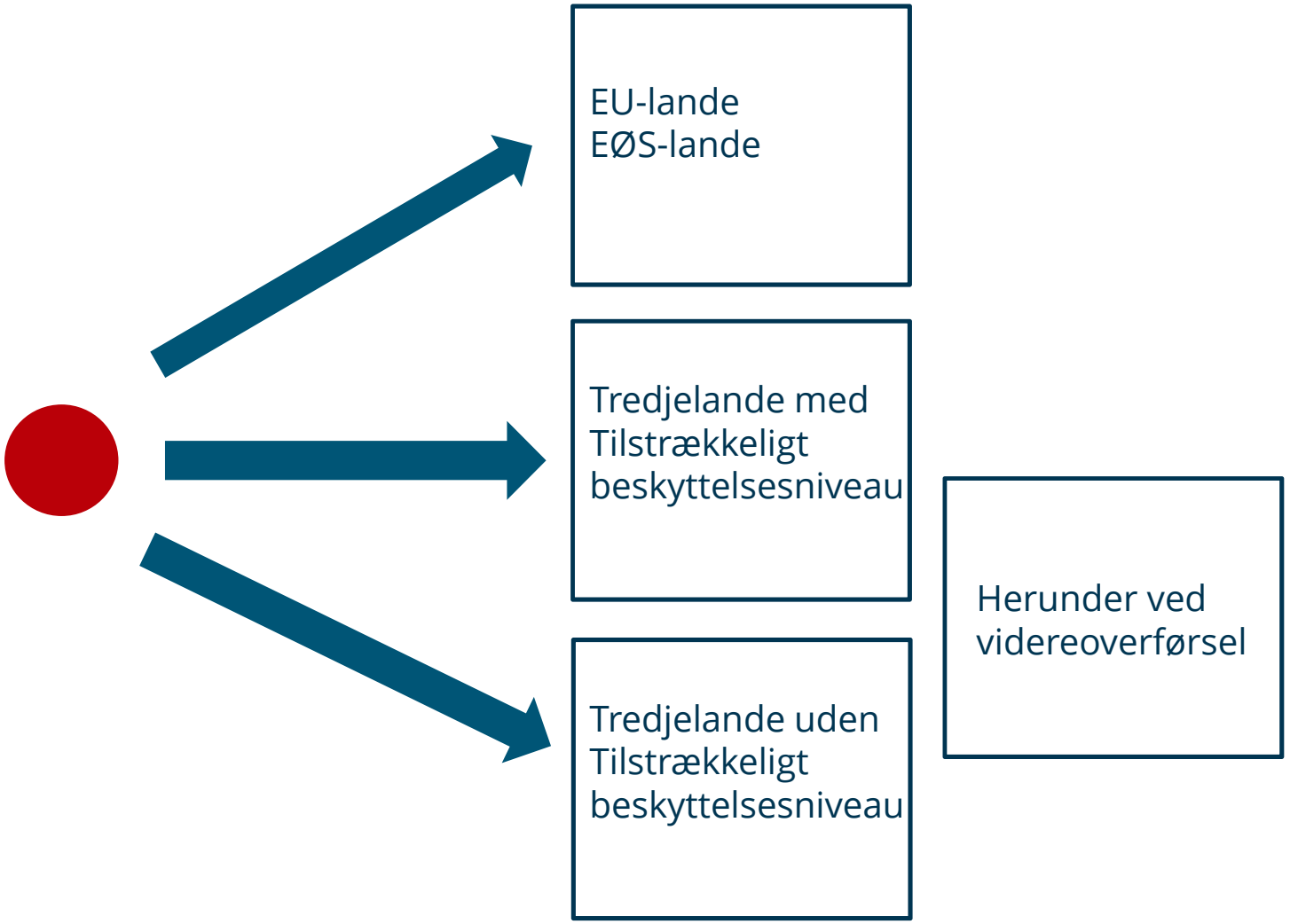

Overførsel
Videregivelse
til 3. mand
Intern anvendelse
Overladelse
til databehandler

'De tre dimensioner'

Eksempler på behandling i en koncern
- fx personaleoplysninger



3 mulige overførsler



Sikre tredjelande

- Kommissionen træffer afgørelse om et tredjelands status
- På baggrund af "beskyttelsesniveauets tilstrækkelighed"
- Hvilke lande er det?

Usikre tredjelande

- Kræver de "fornødne garantier"
- Uden krav om tilladelse fra Datatilsynet
  - BCR
  - Kommissionens standardbestemmelser
  - En godkendt code of conduct
  - En godkendt certificeringsmekanisme
  - Bindende instrumenter mellem offentlige organer
- Krav om tilladelse fra Datatilsynet
  - Ad hoc kontraktbestemmelser
  - Generelt krav om transparens
- Andre tilfælde
  - En dom eller afgørelse, som kan håndhæves i kraft af en international aftale eller traktat
  - Samtykke eller opfyldelse af en kontrakt med den registrerede eller i dennes interesse
  - Samfundsinteresser eller retskrav
  - One-off og ikke grundlag i andre bestemmelser og få registrerede og vægtige interesser

BECH-BRUUN

HR og persondata

Persondatalovgivning i ansættelsesforhold?

- Der er ikke nogen systematisk lovgivning om behandling af personoplysninger i ansættelsesforhold
  - Forskelsbehandlingsloven – forbud mod behandling af oplysninger om race, hudfarve, religion eller tro, politisk anskuelse, seksuel orientering, national, social eller etnisk oprindelse.
  - Helbredsoplysningsloven – begrænser adgang til at indsamle og benytte informationer om lønmodtageres helbredsmæssige forhold
  - Regler om whistleblowing (FIL §§ 75 a og 75 b, hvidvaskdirektiv)

- Mange spørgsmål om behandling af medarbejderoplysninger må håndteres inden for rammerne af generelle arbejdsretlige principper (især ledelsesretten)
- Behandling af medarbejderoplysninger er stort set heller ikke reguleret via kollektive overenskomster (dog visse retningslinjer for fx kontrolforanstaltninger)
- Persondataloven → Databeskyttelsesloven/databeskyttelsesforordningen

Forskellige kategorier af personoplysninger

Kategori 1: Følsomme oplysninger

- Oplysninger om fagforeningsmæssige tilhørsforhold, helbredsmæssige forhold, politisk, religiøs eller filosofisk overbevisning, seksuelle forhold, racemæssig eller etnisk baggrund (udtømmende opregning)
    - Forordningen → genetiske data og biometriske data med det formål entydigt at identificere en person

Kategori 2: Semi-følsomme oplysninger (udgår med forordningen)

- Oplysninger om "strafbare forhold", "væsentlige sociale problemer" og andre "rent private forhold" (fx bortvisning fra jobbet og resultater af personlighedstestning)

Kategori 3: Almindelige oplysninger

- ID-oplysninger, økonomi, skat, gæld, sygedage, tjenstlige forhold, familieforhold, bolig, bil, eksamen, ansøgning, CV, ansættelsesdato, stilling, arbejdsområde, arbejdstelefon, stamoplysninger: navn, adresse, fødselsdato

Kategori 4: Cpr-nr.

Eksempel personalemappe

"Enhver form for information om en identificeret eller identificerbar fysisk person"			
Jens Jensen Salgsdirektør Ansat siden 2001 Gift med Lotte på 3. år, har 2 børn Bor i Charlottenlund Har haft 13 sygedage i år	Gennem en skilsmisse for 5 år siden Entusiastisk personlighedstype ifølge Meyers Briggs Social Styles analyse	Lider af kronisk hovedpine Medlem af DJØF Har stress-symptomer og et alvorligt alkoholmisbrug	CPR. Nr. 120571-1111
Almindelige	Semifølsomme	Følsomme	Personnummer

BECH-BRUUN

Før ansættelse

Indsamling af oplysninger om jobansøgere

- Kun oplysninger, som er relevante for at kunne vurdere kandidatens egnethed til stillingen, må indsamles/behandles.
- For alm. oplysninger: behandlingen foregår på den registreredes anmodning forud for indgåelsen af en kontrakt (Art. 6, stk. 1, litra b) .
- Straffeattester: samtykke (Art. 10, stk. 1 + kriminalregisterbekendtgørelsen) (arbejdsgiver kan ikke kræve straffeattest af samtlige jobansøgere, jf. Datatilsynets udtalelse af 15/10-2010 og FOB 19/4-2011)

Samtykke til behandling af oplysninger om jobansøgere

- Behandlingen skal overholde de almene persondataretlige principper i Art. 5, selvom den berørte har givet samtykke
  - Saglighedskrav til arbejdsgiveres anvendelse af personoplysninger

BECH-BRUUN

Arbejdsgiverens indsamling af oplysninger om jobansøgere

- Ledelsesretten giver som udgangspunkt arbejdsgiveren adgang til at ansætte medarbejdere efter et frit skøn

- Arbejdsgiveren kan:

1. Anmode ansøgeren om alle oplysninger, som må anses for relevante for det konkrete arbejde, fx straffeattest.
2. Selv søge informationer på anden vis om ansøgeren, fx via Google, LinkedIn og Facebook.
3. Kontakte tidligere arbejdsgivere, som ansøgeren selv har oplyst i ansøgningen (referencepersoner).

Særligt om oplysninger på en åben/lukket profil – fx Facebook

- For så vidt angår sociale medier er det relevant, hvornår en oplysning er offentliggjort
- Personoplysninger offentliggjort af medarbejderen kan frit behandles, jf. fx Art 9, stk. 2, litra e)
- Oplysninger på en åben profil anses for offentliggjort, da en bredere kreds af personer har haft mulighed for at opnå kendskab til oplysningerne
- På en lukket profil med et begrænset antal venner anses oplysningerne ikke for offentliggjort i persondatalovens forstand

Oplysningspligt og slettepligt

- Der er oplysningspligt efter Art. 13-14
- Informationsindsamling, der foregår via sociale medier og andre netbaserede kilder er omfattet af oplysningspligten, medmindre ansøgeren allerede er bekendt med oplysningerne

- Slettepolitik – opbevaring op til 6 måneder efter stillingen er besat?

BECH-BRUUN

Under ansættelsen

BECH-BRUUN

Oplysninger om medarbejderens sygefravær

Helbredsoplysninger er følsomme oplysninger i persondataretlig forstand →

- Samtykke fra medarbejder til at registrere oplysningen på personalesagen
- Forpligtelse i henhold til lovgivning eller kollektiv overenskomst
- Beskyttelse af retskrav (retssag / dagpengerefusion)

BECH-BRUUN

Offentliggørelse af oplysninger om medarbejderen

- Arbejdsgiveren kan offentliggøre relevante arbejdsrelaterede informationer om de ansatte

- Der er videre adgang til at offentliggøre data via intranet end internet
  - OBS! Koncernselskaber uden for EU/EØS

- Offentliggørelse af de ansattes private forhold kræver som udgangspunkt samtykke, fx foto, privatadresse eller privat e-mail

- En arbejdsgiver må ikke – via intranet eller opslagstavle – uden videre orientere medarbejderne om enkeltmedarbejderes

  a) antal sygedage eller

  b) opsigelsesgrunde

BECH-BRUUN

Gennemgang af medarbejderens internetbrug

Hovedregel: Der skal indhentes samtykke

- Foreligger der for arbejdsgiveren en berettiget interesse, som overstiger hensynet til medarbejderen?

Uden samtykke:

- Gennemgang af fx internetbrowser og e-mails for at undersøge mistanken om misbrug eller for at få adgang til arbejdsrelaterede informationer

<u>Typiske saglige formål ved gennemgang af medarbejderes brug af internet</u>

- Tekniske og sikkerhedsmæssige hensyn – drift, sikkerhed, genetablering og dokumentation
- Kontrol af medarbejderes brug af internet – det er i hvert fald et sagligt formål at undersøge, om virksomhedens systemer er blevet misbrugt til private formål i strid med virksomhedens politik

Overvågning af e-mails

- Ulovligt at gøre sig bekendt med private e-mails efter straffeloven
- Generel sikkerhedskopiering er tilladt
- Mulighed for gennemgang af arbejdsrelaterede e-mails ved fravær eller lign.
- Gennemgang af arbejdsmails tilladt, hvis bestyrket mistanke om brud på interne forskrifter om sikkerhed eller brug af e-mail
- Overvågning skal være varslet
- Etablér politik på området

- **Højesteretsdom af 4. februar 2015 (189/2013)**

Skærpede sikkerhedskrav til HR-oplysninger (1)

Det er en betingelse for tilladelse til personaleadministration, at virksomheden lever op til sikkerhedskravene:

1. Beskrivelse af beskyttelse af personaleoplysninger og implementering af minimumskrav
2. Begrænset adgang – sagligt behov
3. Instruktion og oplæring
4. Aflåst fysisk opbevaring
5. Adgangskoder
6. Registrering af forgæves adgangsforsøg
7. Beskyttelse af personaleoplysninger på USB-nøgler
8. Firewall og viruskontrol

Skærpede sikkerhedskrav til HR-oplysninger (2)

9. Kryptering af hjemmesideformularer, hvor følsomme personaleoplysninger og personnummer kan indtastes og fremsendes.
10. Kryptering anbefales, hvis følsomme personaleoplysninger og personnummer sendes med e-mail via internettet.
11. Der skal træffes fornødne foranstaltninger, så oplysninger ikke kan komme til uvedkommendes kendskab i forbindelse med reparation og service, salg eller kassering af dataudstyr.
12. Skriftlige databehandleraftaler.

BECH-BRUUN

Efter ansættelsen

Oplysninger om den fratrådte medarbejder

- Slettepolitik – opbevaring op til 5 år efter fratrædelse?
  - Løbende oprydning i personalemappen

BECH-BRUUN

Interne privacy politikker

Privacy politikker

- Information om hvordan den dataansvarlige behandler de personoplysninger, som den dataansvarlige indsamler om de registrerede personer
- Informationen gives til, fx
  - Ansatte
  - Kunder
  - Leverandører
  - Brugere
  - Besøgende
  - Medlemmer
  - Borgere

→ På baggrund af informationen skal den registrerede være i stand til at vurdere eventuelle risici forbundet med afgivelsen af personoplysninger

Særligt vedr. behandling af personoplysninger om medarbejdere

- Ansatte er ”registrerede” og har derfor samme rettigheder, og arbejdsgiveren skal derfor opfylde sine forpligtelser som dataansvarlig
  - Udarbejdelse af særskilt HR-persondatapolitik (opfylde oplysningspligten)
  - Eksisterende ansættelseskontrakter, personalepolitikker, samtykkeerklæringer, som indeholder bestemmelser om personoplysninger (tv-overvågning, e-mail- og internetpolitik, whistleblowerpolitik mv.) skal gennemgås/udarbejdes og ajourføres
  - Medarbejdere, som behandler personoplysninger, skal underlægges særlige fortrolighedsklausuler (fortrolighed og tavshedspligt) – gælder fx medarbejdere i HR og DPO’en

BECH-BRUUN

Persondataforordningen

Overholdelse af arbejdsretlige forpligtelser

Databeskyttelseslovens § 12, stk.1, 2 og 3

- Stk. 1: Juridisk grundlag til behandlingen af medarbejderoplysninger, hvis det er nødvendigt for overholdelse af arbejdsretlige forpligtelser eller rettigheder, som er fastlagt i kollektiv overenskomst eller anden lovgivning

- Stk. 2: Juridisk grundlag til behandlingen af medarbejderoplysninger, hvis behandlingen har sin baggrund i (ikke er nødvendiggjort af) en kollektiv overenskomst eller anden lovgivning

  → **interesseafvejningsregel**

- Stk. 3: Samtykke

Skærpede krav til samtykke

Samtykke som behandlingsgrundlag:

Kategori 1: Almindelige oplysninger: Samtykke

Kategori 2: Følsomme oplysninger: Udtrykkeligt samtykke

- En dataansvarlig skal altid kunne dokumentere at have modtaget den registreredes samtykke til behandling af personoplysninger
- Samtykke kan ikke udgøre lovligt behandlingsgrundlag, hvis der er en klar ubalance mellem datasubjektet og den dataansvarlige – særhjemmel i databeskyttelseslovens § 12, stk. 3.
- Vurdering af, om et samtykke er frivilligt: Samtykke som betingelse for tillægsydelser, der ikke er nødvendige i forhold til en kontrakt?
- Det skal være lige så let at trække et samtykke tilbage som at afgive det
- Hvis samtykke indhentes igennem en skriftlig erklæring med anden information – fx en ansættelseskontrakt eller en privacy policy – skal samtykkeanmodningen adskilles tydeligt fra øvrigt indhold

BECH-BRUUN

Praktisk compliance og "accountability"

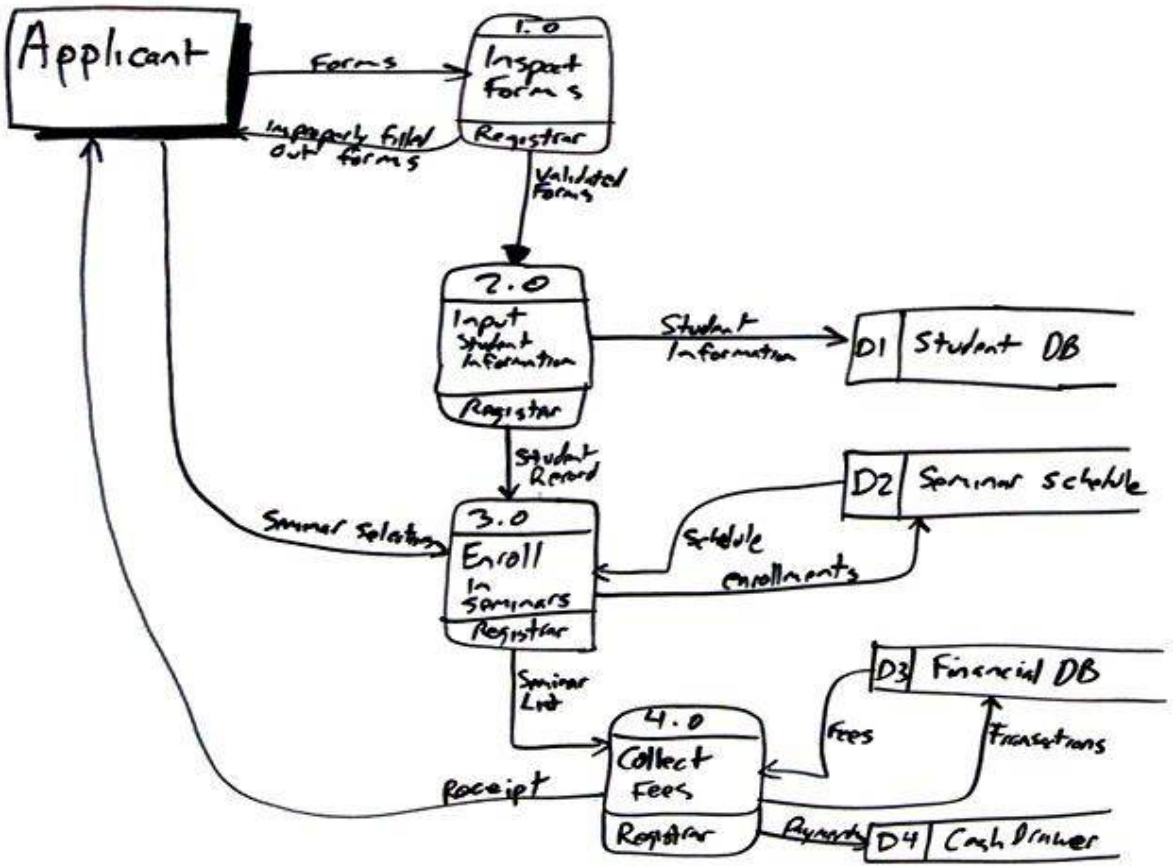
BECH-BRUUN

Vores projekttilgang

Kort fortalt, så anbefaler vi organisationer at gribe projektet an i 5 faser.

1	**Foranalyse:**	Afklare og vurdere organisationens risikobillede. Styringsværktøj til prioritering af projekt og indsats
2	**Planlægning:**	Mandat, målsætning, plan og ressourcer (både intern og eksternt) til projektet
3	**Analyse:**	Den centrale analyse- og dokumentationsfase. Metodisk afdækning af persondatabehandlinger
4	**Implementering:**	Prioritering og gennemførelse af alle de øvrige tiltag for at sikre compliance
5	**Drift og rapportering:**	Complianceprogrammet i drift. Sikre ledelse, monitorering og rapportering

Hvad er (person-)datastrømme?
(Man risikerer at få svar som man spørger!)

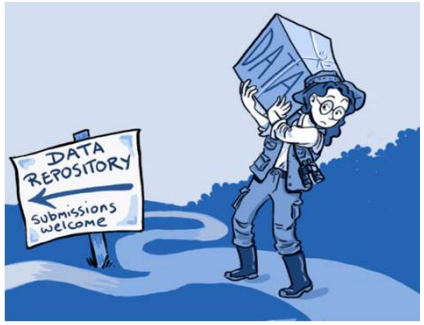


Effekten af en god analyse af persondatastrømme

- Overblik over væsentligste behandlinger af persondata i organisation
- Grundlag for compliance med kravene i persondataforordningen
- Mulighed for at optimere processer med behandling af personoplysninger

Analyse af persondatastrømme – hvordan gør man?

- Interviews
- Spørgeskemaer
- Tænke dynamisk – ingen persondatastrømme er statiske
- Datamodel – hvordan struktureres mængden af input?
- Konsolidering i database/applikation/ Excel/andet?



Roche DG, Lanfear R, Binning SA, Haff TM, Schwanz LE,

Kravene om "accountability" og "fortegnelser over behandlingsaktiviteter

- Den dataansvarlige er ansvarligt for og skal kunne påvise, at principperne for behandling af personoplysninger overholdes ("Accountability") (Art. 5, stk. 2)
- Den dataansvarlige skal kunne dokumentere compliance med forordningen (Art. 24)
- Både dataansvarlige (og databehandlere) skal opbevare dokumentation for enhver behandling af personoplysninger (gælder ikke for virksomheder med under 250 ansatte, med mindre…) (Art. 30)
- Dokumentationen skal mindst omfatte:
  - Navn og kontaktinfo. på den dataansvarlige. Hvis relevant også på fælles dataansvarlige, evt. repræsentant samt DPO
  - Formålene med behandlingen
  - Beskrivelse af kategorier af registrerede og kategorier af personoplysninger
  - Kategorier af modtagere af personoplysningerne
  - Evt. overførsel af personoplysninger til et tredjeland, herunder identifikation af dette tredjeland, og dokumentation af fornødne garantier ved overførsel til ikke-sikre tredjelande
  - *Hvis muligt*, en generel angivelse af tidsfristerne for sletning af de forskellige kategorier af personoplysninger
  - *Hvis muligt*, en beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger
- Fortegnelser skal foreligge skriftligt (elektronisk) og stilles til rådighed for tilsynsmyndigheden efter anmodning

Overvejelser inden opgaven gribes an

- Hvad er en behandling af personoplysninger?
- Hvordan adskiller man datastrømme fra persondatastrømme?
- Kan I fastsætte formålene med nogle af de konkrete behandlinger af personoplysninger, som foregår i jeres organisation?
- Kan I beskrive kategorier af registrerede i jeres organisation?
- Kan I beskrive kategorierne af personoplysninger i jeres organisation?
- Kan I beskrive kategorier af modtagere, som personoplysninger er eller vil blive videregivet til (herunder tredjelande eller internationale organisationer) i jeres organisation?
- Kan I beskrive de forventede tidsfrister for sletning af de forskellige kategorier af oplysninger, hvis muligt, i jeres organisation?
- Er det muligt generelt at beskrive de tekniske og organisatoriske sikkerhedsforanstaltninger i jeres organisation?

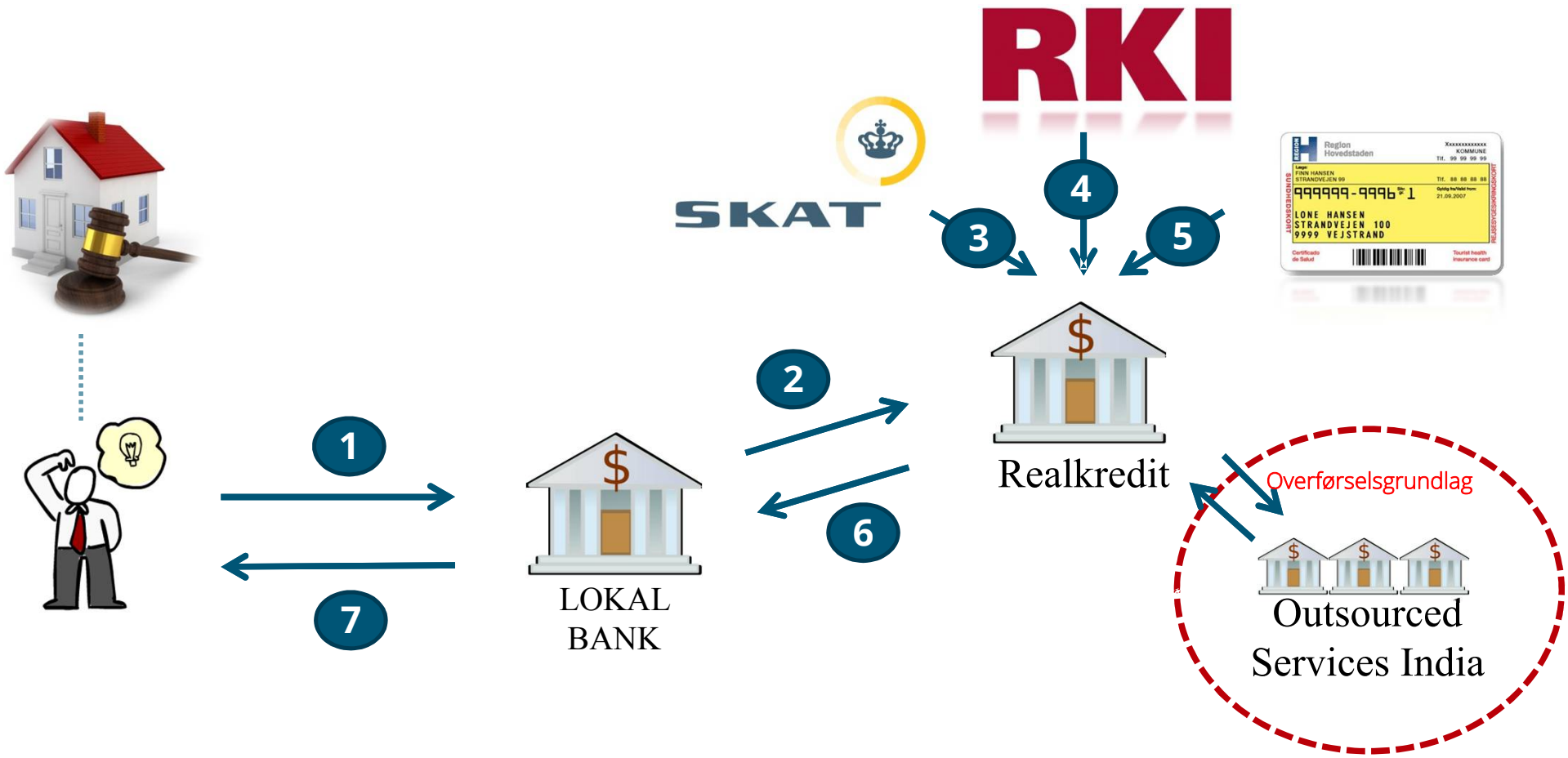
BECH-BRUUN

Hvor ”gemmer” personoplysninger sig?

- Personoplysninger indgår i mange forretningsprocesser
- Hver organisation har egne processer - der bør undersøges, kortlægges og risikovurderes
- Processer understøttes af forskellige systemer, der kan indeholde personoplysninger

Human Resource Systems	Customer Relation Management (CRM)	Sales systems	Supplier/Vendor Relation Management Systems (SRM)	Enterprise Resource Management (ERM)
Content Management Systems (CMS)	Marketing/ targeting systems	Travel Management systems, and ancillary systems e.g cost reporting	Financial reporting systems	Business Intelligence systems
Physicalaccess management systems	Video Surveillance systems	Whistleblower system	Shadow IT systems	Analogue processing of personal data (Fillngcabinets, binders)

Forretningsproces: Hvad så når nye forhold tilføjes?



Spørgeskema

- Proces
  - *Grundlæggende oplysninger om processen, fx formål og procesejer*
- Registrerede
  - *Kategorier af registrerede*
- Kategorier af personoplysninger
  - *Hvilke typer af oplysninger, fx følsomme personoplysninger*
- IT-værktøjer og fysiske arkiver
  - *Hvilke IT-værktøjer og fysiske arkiver indgår i processen. Er IT-værktøjet risikovurderet*
- Overførsel til eller fra eksterne enheder
  - *Overføres der til eksterne enheder/tredjeparter udenfor koncernen; land, formål med og retsgrundlag for overførsel*
- Overførsel til eller fra koncernenheder (datterselskaber)
  - *Hvilke enheder overføres der til; land, formål med og retsgrundlag for overførsel*

BECH-BRUUN

Compliance nu og fremover

Implementering - formelle krav

Indhente samtykke til behandling – gode råd

- Skab overblik over, hvor samtykker eksisterer internt og eksternt.
- Er interne processer i stand til at styre samtykke? Fx tilbagetrækning.
- Adskil samtykker fra andre dokumenter, fx bilag til ansættelseskontrakt.

Implementering - formelle krav

Sikkerhedsbrud

- Anmeldelse af et sikkerhedsbrud – skal ske senest **72 timer** efter er man blevet bekendt med det (art. 33), hvis sikkerhedsbruddet indebærer en risiko.
  - Fx tab af usb-nøgle med kunde-/brugerlister, offentliggørelse via website.

- Anmeldelse **efter** 72 timer – **begrundelse** for forsinkelse skal medsendes.

- I visse tilfælde skal vedkommende, oplysningerne drejer sig om underrettes.

Implementering - formelle krav

Sikkerhedsbrud– gode råd (1)

- Fastlæg hvem i virksomheden/organisationen der skal vurdere og evt. fortage anmeldelsen og sikre opfølgning? (ikke hvis DPO er udpeget)

Til Datatilsynet skal der sammen med anmeldelsen bl.a. sendes:

- De sandsynlige **konsekvenser** af bruddet.
- De foranstaltninger, der træffes for at **håndtere** og **minimere** skadevirkning.

HUSK – I visse tilfælde underretning af personen, der også altid kan rette henvendelse til Datatilsynet med klage.

BECH-BRUUN

Implementering - formelle krav

Sikkerhedsbrud– gode råd (2)

- Sikre god kommunikation til personen, hvis vedkommende skal underrettes.
- Beskrive i politik, hvordan det håndteres – roller og ansvar fordeles.
- Overveje behov for på forhånd at lave anmeldelses – og underretningsskabeloner.
- Huske muligheden for trinvis levering af data, når ikke muligt at give oplysninger samlet.

Implementering - formelle krav

Håndtering af indsigtsanmodninger

Kunde/bruger har ret til at få bekræftet, **om** personoplysninger behandles og få **adgang til informationen** og en række andre oplysninger.

BECH-BRUUN

Implementering - formelle krav

Håndtering af indsigtsanmodninger – gode råd

- Test om I kan finde alt frem – er infrastrukturen og processerne på plads?
- Kan det gøres hurtigt og effektivt med så lidt kommerciel/driftsmæssig ulempe som muligt?
- Beskrive i politik, hvordan det håndteres – roller og ansvar fordeles.
- Overveje behov for på forhånd at lave svarskabeloner?

Implementering - dokumentation

Dokumentation mv.

- Fortegnelse.
- Politikker og procedurer.

BECH-BRUUN

Kontakt

Thorsten Kranz

Persondataspecialist

IP & Technology

T +45 72 27 33 52
M +45 25 26 33 52
E thkr@bechbruun.com