KROMANN REUMERT

ER DIN VIRKSOMHED KLÆDT PÅ TIL DEN NYE PERSONDATAFORORDNING?

Udvalgsmøde hos Den Danske Fondsmæglerforening
14. november 2016

Tina Brøgger Sørensen, partner, advokat

KROMANN REUMERT

AGENDA

- Velkomst og introduktion
- Den juridiske baggrund for complianceprogrammet
  - Kort introduktion til den gældende persondatalov
  - Persondataforordningen - nyskabelser
- Persondataretlig compliance hos din virksomhed
  - Hvilke (overordnede) aktiviteter skal der gennemføres?
  - Hvordan organiseres arbejdet?
  - Hvilke ressourcer kræver det i virksomheden?

KROMANN
REUMERT

DEN JURIDISKE BAGGRUND FOR COMPLIANCEPROGRAMMET

Hvad handler det om?

SUNDKROGSGADE 5, DK-2100 KØBENHAVN Ø CVR. NR: DK 62 60 67 11

KROMANN REUMERT

PERSONOPLYSNINGER: **ENHVER FORM** FOR INFORMATION OM EN **IDENTIFICERET** ELLER **IDENTIFICERBAR** **FYSISK PERSON** (DEN REGISTREREDE)

- *Persondatalovens § 3, nr. 1*

KROMANN
REUMERT

[…] VED **IDENTIFICERBAR** FYSISK PERSON FORSTÅS EN FYSISK PERSON, DER **DIREKTE ELLER INDIREKTE KAN IDENTIFICERES**, NAVNLIG VED EN **IDENTIFIKATOR** SOM F.EKS. ET NAVN, ET IDENTIFIKATIONSNUMMER, LOKALISERINGSDATA, EN ONLINEIDENTIFIKATOR ELLER **ET ELLER FLERE ELEMENTER, DER ER SÆRLIGE FOR DENNE FYSISKE PERSONS** FYSISKE, FYSIOLOGISKE, GENETISKE, PSYKISKE, ØKONOMISKE, KULTURELLE ELLER SOCIALE **IDENTITET**

- *Persondataforordningens art. 4, nr. 1*

KROMANN REUMERT

BEHANDLING: **ENHVER OPERATION** ELLER RÆKKE AF OPERATIONER **MED ELLER UDEN BRUG AF ELEKTRONISK DATABEHANDLING**, SOM OPLYSNINGER GØRES TIL GENSTAND FOR

- *Persondatalovens § 3, nr. 2*

KROMANN REUMERT

BEHANDLING: **[…]** F.EKS. **INDSAMLING, REGISTRERING, ORGANISERING, SYSTEMATISERING, OPBEVARING**, TILPASNING ELLER ÆNDRING, GENFINDING, SØGNING, BRUG, **VIDEREGIVELSE VED TRANSMISSION,** FORMIDLING ELLER ENHVER ANDEN FORM FOR **OVERLADELSE**, **SAMMENSTILLING** ELLER **SAMKØRING**, BEGRÆNSNING, SLETNING ELLER TILINTETGØRELSE

- *Persondataforordningens art. 4, nr. 2*

KROMANN
REUMERT

GRUNDLÆGGENDE PERSONDATARET

SUNDKROGSGADE 5, DK-2100 KØBENHAVN Ø

CVR. NR: DK 62 60 67 11

KROMANN REUMERT

INTRODUKTION TIL PERSONDATALOVEN

- PDL § 5 – artikel 6 i forordningen
  - God databehandlingsskik – ”lovlighed, rimelighed og gennemsigtighed”
  - Udtrykkelige og saglige formål
  - Proportionalitet
  - Ajourføring, kontrol for at sikre, at der ikke behandles urigtige eller vildledende oplysninger, sletteplig og berigtige
  - Opbevaringsperioden
- Behandlingshjemmel i § 6, § 7 eller § 8 – artikel 6 og 9 i forordningen
- Registreredes rettigheder – artikel 12 ff. i forordningen
  - Oplysningspligt ved indsamling, indsigtsret, indsigelse, tilbagekaldelse af samtykke mv.
- Anmeldelse af behandlinger til Datatilsynet – afskaffelse?

KROMANN REUMERT

GRUNDLÆGGENDE BEHANDLINGSREGLER

- **God databehandlingskik** - § 5
- Saglige og legitime formål - skal angives udtrykkeligt
- Senere behandling må ikke være uforenelig med de oprindelige formål
- Kun relevante og tilstrækkelige oplysninger
- Kun hvis behandlingen er nødvendig
  - Blot fordi den registrerede har offentliggjort sine oplysninger, f.eks. på Facebook, betyder det ikke, at de godt må behandles!
- Proportionalitetsprincippet
- Sletteplig
  - Forældelsesloven, bogføringsloven, løbende aftaleforhold, rimelighed m.v.

KROMANN REUMERT

PERSONDATA – KATEGORIER

§ 6	§ 7	§ 8	§ 11
Almindelige oplysninger	**Følsomme oplysninger**	**Oplysninger af rent privat karakter**	**CPR-numre**
› Navn, journal nr. mv. › Kontaktoplysninger › Køn, alder mv. › Interesser › Kundeprofil, købshistorik › Kreditoplysninger mv. › IP adresser *Muligheder for behandling: bl.a. samtykke, kontrakt, interesseafvejningsreglen – kan ofte behandles uden samtykke*	› Race og etnisk baggrund (ikke nationalitet) › Religion › Politisk overbevisning › Fagforeningsforhold › Helbredsforhold › Seksuelle forhold (ikke registreret partnerskab) *Muligheder for behandling: som UP altid samtykke*	› Strafbare forhold › Væsentlige sociale problemer › Andre rent private forhold: personlighedstests, skilsmisse, adoptionsforhold, positive alkohol- eller narkotikatest mv. *Muligheder for behandling: som UP altid samtykke* *evt. en meget streng interesseafvejning*	› Gælder kun for CPR-numre *Muligheder for behandling: samtykke eller bestemt ved lov, afgrænsede muligheder for videregivelse til brug for identifikation*

KROMANN REUMERT

SAMTYKKE: ENHVER FRIVILLIG, SPECIFIK OG INFORMERET VILJESTILKENDEGIVELSE, HVORVED DEN REGISTREREDE INDVILGER I, AT OPLYSNINGER, DER VEDRØRER DEN PÅGÆLDENDE SELV, GØRES TIL GENSTAND FOR BEHANDLING

- *Persondatalovens § 3, nr. 8*
- *NB! Skærpede krav efter forordningens artikel 7*

KROMANN REUMERT

BEHANDLINGSREGLERNE

ALMINDELIGE OPLYSNINGER

- F.eks.: navn, adresse, skattemæssige oplysninger, bankoplysninger, beskæftigelse, købehistorik, kreditoplysninger mv.
- Hjemmel for behandling ⇨ PDL § 6
  - Som udgangspunkt ikke krav om samtykke fra den registrerede
  - Behandling er nødvendig til opfyldelse af aftale, som den registrerede er part i => aftalen udgør hjemmelsgrundlaget
- Behandlingen kræver IKKE anmeldelse og tilladelse fra Datatilsynet
- NB! Særlige regler om behandling af personnumre ⇨ PDL § 11, stk. 2

KROMANN REUMERT

BEHANDLINGSREGLERNE

FØLSOMME OPLYSNINGER

- Oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold
- Hovedregel: forbud mod behandling
- Undtagelse: hjemmel for behandling ⇨ PDL § 7, stk. 2. F.eks.:
  - Udtrykkeligt samtykke
  - Nødvendigt for, at retskrav kan fastlægges, gøres gældende eller forsvares
- Behandlingen kræver i dag forudgående anmeldelse og tilladelse fra Datatilsynet
- Art. 9: *"genetiske data, biometriske data for entydigt at identificere en person"*

KROMANN REUMERT

BEHANDLINGSREGLERNE

PRIVATE OPLYSNINGER

- Oplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold, f.eks. oplysning om bortvisning, medlemskab af foreninger, alvorlige ulykkestilfælde, skilsmisse og personlighedstests
- Hjemmel for behandling ⇨ PDL § 8, stk. 4
  - Hovedregel: krav om udtrykkeligt samtykke
  - Undtagelse f.eks.:
    - Nødvendigt for at varetage berettiget interesse og denne interesse klart overstiger hensynet til den registrerede
    - Nødvendigt ift. retskrav
- Behandlingen kræver forudgående anmeldelse og tilladelse fra Datatilsynet
- Art. 9: opregner IKKE disse private oplysninger ⇨ ”almindelige oplysninger”

KROMANN REUMERT

KONCERNFORHOLD - TREDJELANDSOVERFØRSLER

- Videregivelse i koncernforhold betragtes som videregivelse til *tredjemand* ⇔ krav om sagligt formål, hjemmel til videregivelse (f.eks. samtykke eller interesseafvejningsreglen) mv.

- Særlige krav ved videregivelse til *tredjelande*, dvs.
  - lande uden for EU,
  - lande, der ikke er omfattet af EØS-samarbejdet, og
  - lande, der ikke er særligt godkendt som et tredjeland med *tilstrækkeligt beskyttelsesniveau*
    - Eksempler på særligt godkendte lande: Israel, Schweiz og Argentina – *forordningen opretholder sådanne godkendelser, indtil de bliver ændret, erstattet eller ophævet ⇨ videregivelse kræver stadig ikke specifik godkendelse*

KROMANN REUMERT

BRUG AF DATABEHANDLERE

Særlige krav

- Skriftlig aftale
- Krav til indholdet:
  - *kun efter instruks fra den dataansvarlige*
  - *databehandleren skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven mv.*
  - *hvis databehandleren er etableret i et andet EU-land, skal de lokale krav om datasikkerhed også være gældende*
- Den dataansvarlige skal sikre sig, at databehandleren kan træffe de nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger, og påse, at dette sker
- Behandlingen er altid den dataansvarliges ansvar!
  - Brug af cloud-baserede løsninger – særlige sikkerhedskrav
  - Offentlig forvaltning - sikkerhedsbekendtgørelsen

KROMANN REUMERT

DEN REGISTREREDES RETTIGHEDER

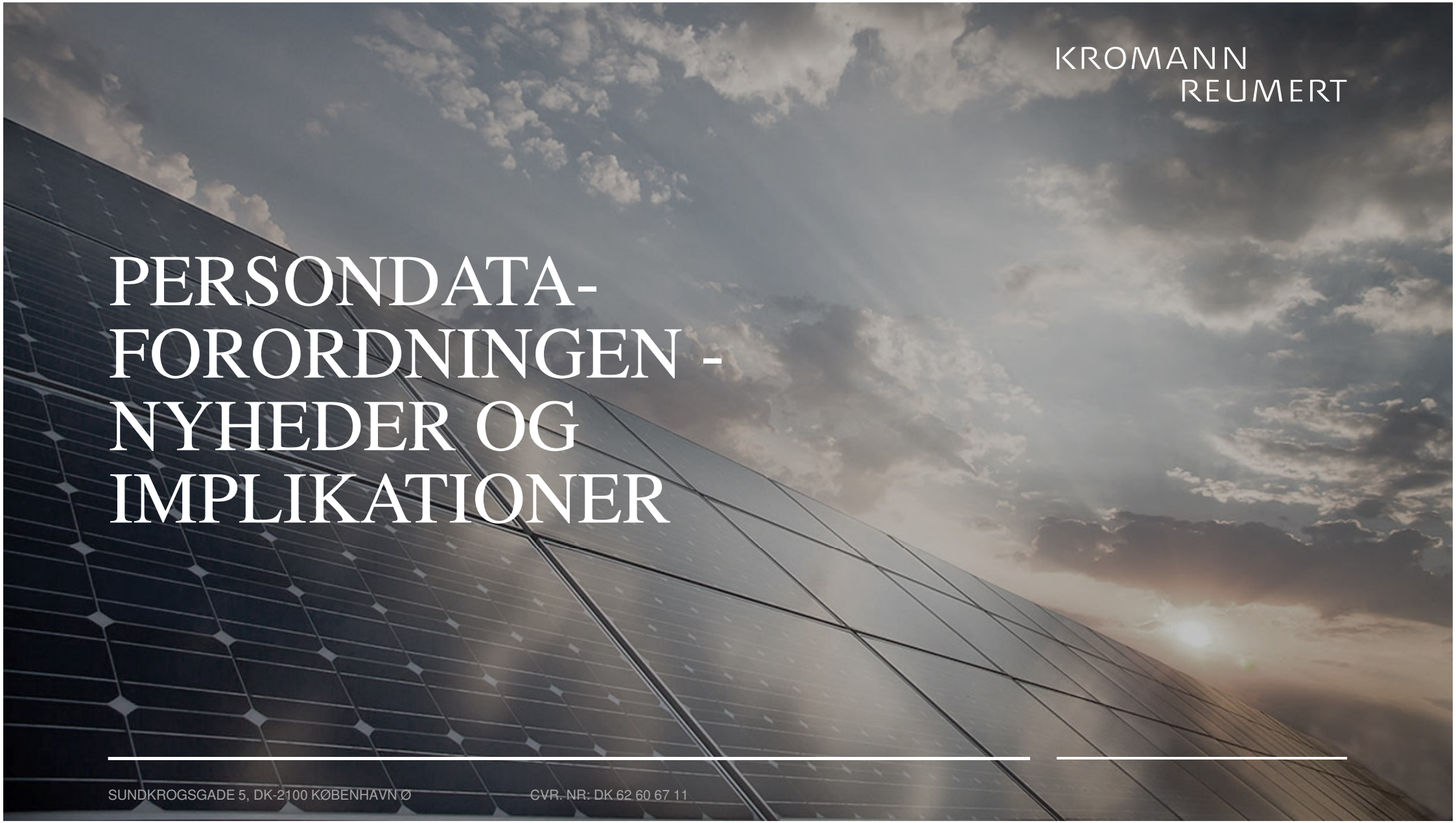
- Oplysningspligt (§§ 28-29)
- Indsigtsret (§ 31)
  - Hver 6. måned
  - Skal på begæring gives skriftligt
  - Kan opkræve 10 kr. pr. påbegyndt side
- Ret til at korrigere og slette oplysninger (§ 37)
  - 3-mand skal underrettes
- Ret til at gøre indsigelse mod behandlingen (§ 35)
- Ret til at tilbagekalde sit samtykke til enhver tid (§ 38)
- Ret til at klage til Datatilsynet (§ 40)

KROMANN REUMERT

ANMELDELSESPLIGT

Lovens UP er anmeldelsespligt, men der er mange undtagelser

- Anmeldelsespligten er tilknyttet bestemte typer behandling
  - Personaleadministration, whistleblowerordninger
  - Følsomme oplysninger
  - Ingen pligt til at anmelde kontrakter
- Forpligtelsen er pålagt den dataansvarlige – databehandlere skal ikke (og kan ikke) anmelde
  - Dog en særlig undtagelse for edb-servicevirksomheder (§ 53-anmeldelse)
    - "driftsafvikling af databehandling for andre udbydes på almindelige markedsvilkår og er virksomhedens egentlige formål"
- Datatilsynets tilladelse afventes, før behandlingen må påbegyndes



KROMANN
REUMERT

PERSONDATA-FORORDNINGEN - NYHEDER OG IMPLIKATIONER

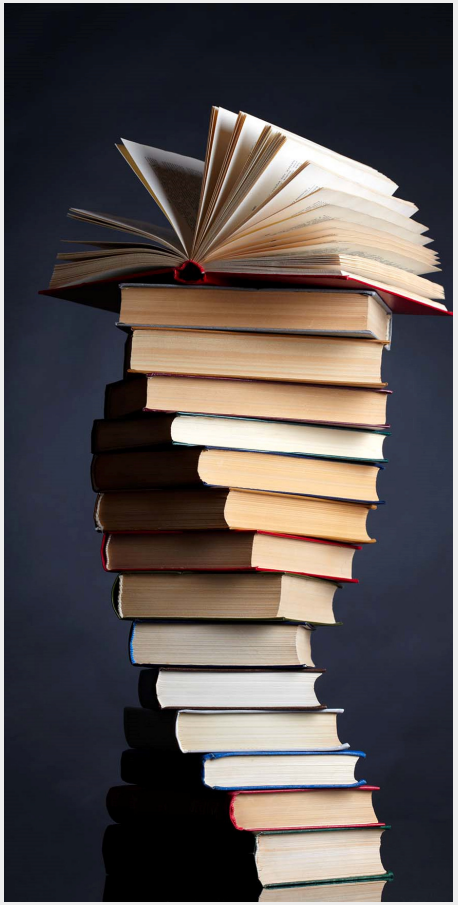
SUNDKROGSGADE 5, DK-2100 KØBENHAVN Ø CVR. NR: DK 62 60 67 11

KROMANN REUMERT

EU-FORORDNING OM DATABESKYTTELSE

- Vedtaget i Europa-Parlamentet den 14. april 2016
- Anvendelsesfrist den **25. maj 2018**

- Overordnede ønsker er bl.a.
  - Ensartede regler i EU
  - Skærpet beskyttelse af *fysiske* personer
  - Hårdere sanktioner
    - Administrative bøder på op til EUR 10 mio. / 20 mio. eller for en virksomhed med op til 2 % / 4% af den samlede globale årlige omsætning i det foregående regnskabsår, såfremt dette beløb er højere



KROMANN REUMERT

EU-FORORDNING OM DATABESKYTTELSE

- Udeståender
  - Hvilke specifikke bestemmelser fastsættes i Danmark?
    - Se f.eks. artikel 37, stk. 4:
      - *"I andre tilfælde end de i stk. 1 omhandlede, kan eller, når det kræves i henhold til EU-retten eller medlemsstaternes nationale ret, **skal** den dataansvarlige eller databehandleren….., udpege en databeskyttelsesrådgiver…".*
  - Kommissionen kan vedtage delegerede retsakter
  - Fortolkningsbidrag fra
    - Det Europæiske Databeskyttelsesråd
    - Justitsministeriet
    - Datatilsynet

KROMANN REUMERT

EU-FORORDNING OM DATABESKYTTELSE

- EKSEMPLER PÅ NYSKABELSER:
- **1. Udvidelse af det territoriale anvendelsesområde** (art. 3)
  - Gælder for etablerede i EU, *uanset* om behandlingen finder sted i EU eller ej
  - Gælder uanset om dataansvarlig/databehandler er etableret i EU, hvis registrerede er i EU
    - F.eks. online salg af produkter eller web-baserede ydelser, eller online eller mobil tracking af fysiske personer, der er i EU

- **2. Dokumentationskrav** og **DPOs** (art. 24, art. 30 og art. 37 ff.)
  - Skifte fra anmeldelsessystem til krav om at *påvise* compliance og evt. tillige føre *interne* fortegnelser over behandlingsaktiviteter
  - Visse dataansvarlige/databehandlere har pligt til udpegelse af DPO

KROMANN REUMERT

EU-FORORDNING OM DATABESKYTTELSE

- **3. Privacy by design og privacy by default (art. 25)**
  - Pligt til at indtænke databeskyttelsesprincipper allerede ved design af nye teknologier, produkter og ydelser
  - Standardindstillinger skal sikre, at kun *nødvendige* oplysninger behandles

- **4. Konsekvensanalyse (art. 35)**
  - Pligt hvis en type behandling *"sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder"*
  - Er f.eks. navnlig påkrævet ved vurderinger baseret på automatisk behandling, herunder profilering

- **5. Øget krav om transparens (art. 13-14)**
  - Oplysningspligten ved indsamlingen af personoplysninger

KROMANN REUMERT

EU-FORORDNING OM DATABESKYTTELSE

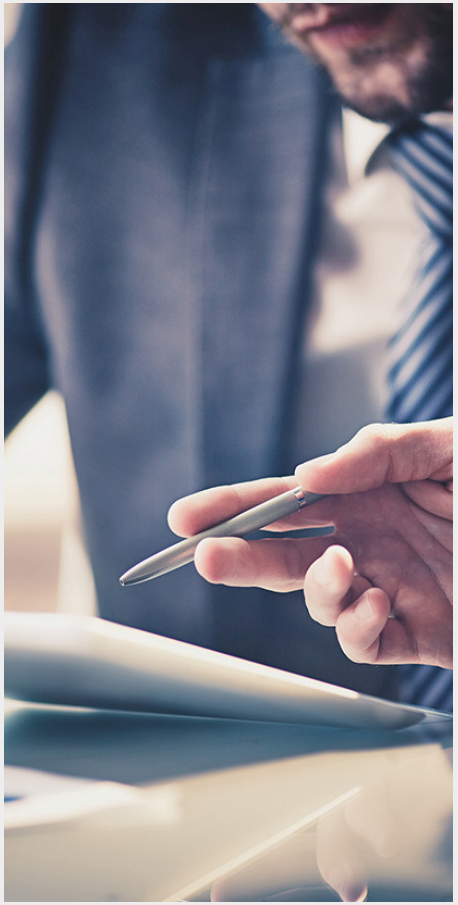
6. Strengere betingelser for samtykke (art. 7), f.eks.

- Inden der gives samtykke, skal den registrerede oplyses om, at samtykket kan trækkes tilbage
- Opfyldelse af kontrakt må ikke være gjort betinget af samtykke til behandling af personoplysninger, der ikke er nødvendig for opfyldelse af kontrakten

› **7. Øgede rettigheder for de registrerede (art. 15 ff.)**

- Indsigsret, ret til berigtigelse, sletning, begrænsning af og indsigelse mod behandling, dataportabilitet mv.

› **8. Pligt til anmeldelse af brud på persondatasikkerheden (art. 33)**



KROMANN REUMERT

EU-FORORDNING OM DATABESKYTTELSE

- **9. One-stop shop (art. 56)**
  - Én ledende tilsynsmyndigheds kompetence ved grænseoverskridende behandling

- **10. Databehandlere**
  - Strengere krav til indholdet af den pligtige databehandleraftale (art. 28)
  - Erstatningsansvar over for skadelidte for skade forvoldt af denne (art. 82)
  - Kan pålægges bøde for overtrædelse af forordningen (art. 83)

PERSONDATARETLIG COMPLIANCE - HVAD SKAL DIN VIRKSOMHED GØRE?

SUNDKROGSGADE 5, DK-2100 KØBENHAVN Ø CVR. NR: DK 62 60 67 11

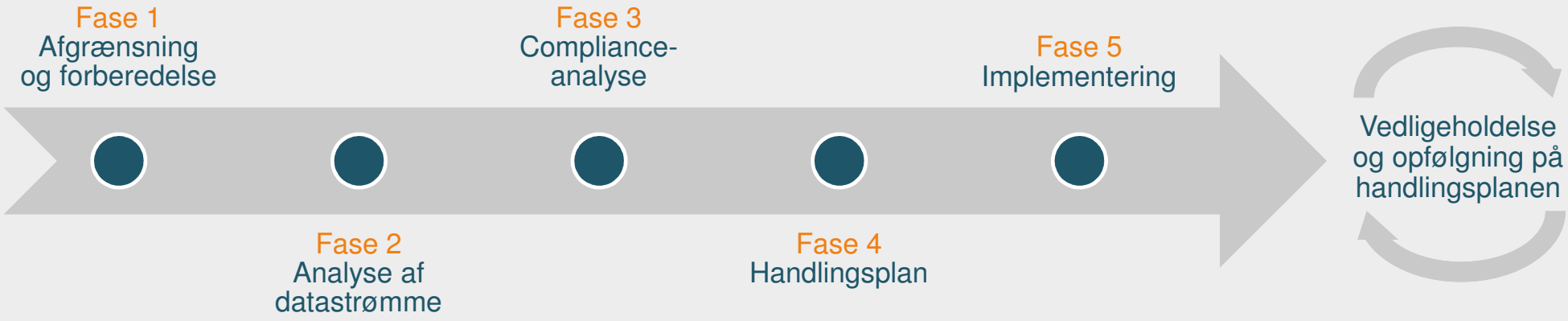
KROMANN REUMERT

12 SPØRGSMÅL – INSPIRATION FRA DATATILSYNET

- Har I kendskab til den nye databeskyttelsesforordning?
- Hvilke personoplysninger behandler I?
- Hvilken information giver I de registrerede?
- Hvordan opfylder I de registreredes rettigheder?
- På hvilket retligt grundlag behandler I personoplysninger?
- Hvordan indhenter I samtykke?
- Behandler I personoplysninger om børn?
- Hvad skal I gøre ved brud på persondatasikkerheden?
- Er jeres behandlinger forbundet med særlige risici?
- Har I indtænkt databeskyttelse i jeres it-systemer?
- Hvem er ansvarlige for databeskyttelsesspørgsmål hos virksomheden?
- Driver I virksomhed i flere lande (eller overfører I oplysninger til udlandet)?

KROMANN REUMERT

KROMANN REUMERTS COMPLIANCE-MODEL



KROMANN
REUMERT

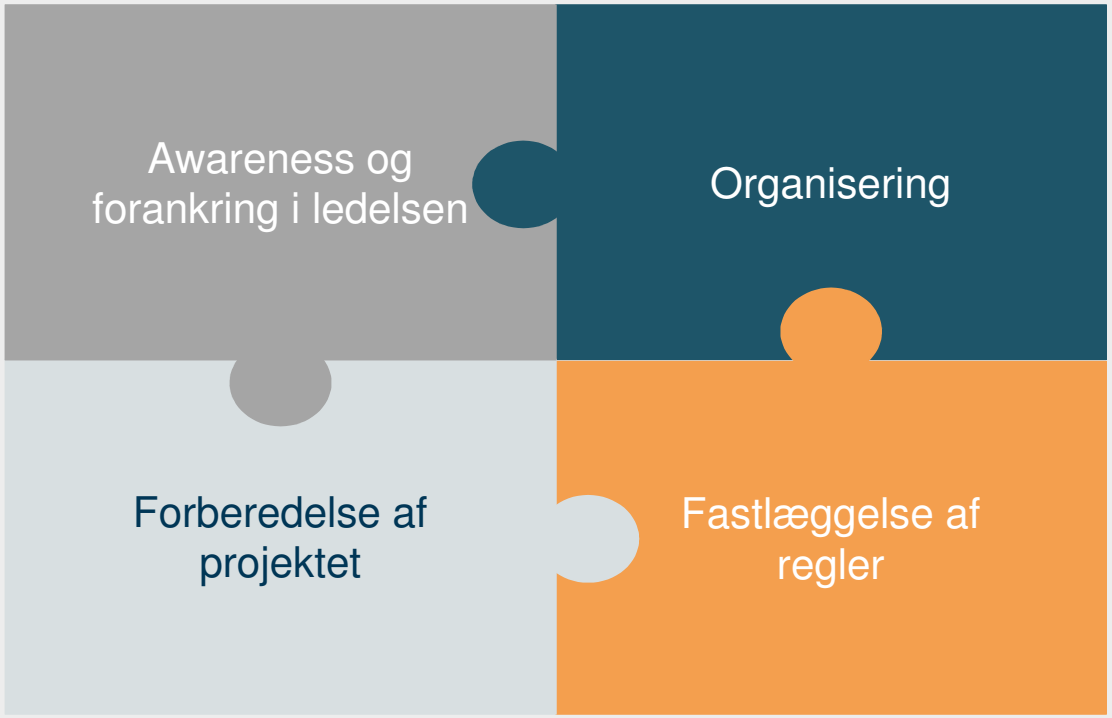
FASE 1
AFGRÆNSNING OG FORBEREDELSE

KROMANN REUMERT

FASE 1 - AFGRÆNSNING OG FORBEREDELSE (1)

Fase 1 skal sætte scenen for compliance-projektet og sikre organisatorisk forankring

- Indledende fase – "***Projektoverblikket***"
- Formålet med fase 1 er at **sikre, at organisationen og projektet bliver klar til at gennemføre de øvrige aktiviteter**
- Forberedelse er afgørende for et velgennemført compliance-program



A1
A2

KROMANN REUMERT

FASE 1 - AFGRÆNSNING OG FORBEREDELSE (2)

Awareness og forankring i ledelsen

- Skab **awareness** om persondataret og compliance i organisationen –særligt på relevante ledelsesniveauer
  - "*Den brændende platform*" - Hvad er persondata, og hvorfor er det vigtigt?
- Sørg for **forankring i ledelsen**
  - Opbakning og prioritering
  - Budget – både penge og timer
  - **Placering af det organisatoriske ansvar** – hvem har det overordnede ansvar?
- Skab en **vision og et mål** for projektet – hvad vil I opnå?

Organisering

- Etabler en **hensigtsmæssig organisation** til gennemførsel af compliance-projektet
- Sørg for at have de **nødvendige ressourcer og kompetencer** til projektet:
  - **Jura** – men det er ikke (kun) et juridisk projekt
  - **IT** / **IT-sikkerhed**
  - **Forretningen**
  - **Ledelseskontakt** (evt. i form af styregruppe el.lign.)
  - **Andre?** (HR, compliance, marketing mv.)
- Den konkrete organisering afhænger af virksomhedens størrelse, art og organisation
- Afklaring af **ressourcer** og **budget**

Slide nummer 32

A1 Author; 18-09-2016

A2 Author; 18-09-2016

KROMANN REUMERT

FASE 1 - AFGRÆNSNING OG FORBEREDELSE (3)

Forberedelse af projektet

- **Overordnet koordinering** af projektet
  - Realistisk tidsplan for hele projektet og de enkelte faser
  - Forventninger til output af de forskellige faser?
- **Afgrænsning**
  - Afgrænsning af de relevante juridiske enheder og de relevante databehandlingsaktiviteter
  - Afgrænsning af relevante personer til interviews
  - Afklaring af antal IT systemer, der indeholder persondata
- **Afklaring af eksisterende dokumentation**
  - Hvor langt er I allerede?
  - Beskrevne processer, politikker mv.

Fastlæggelse af regler

- **Fastlæggelse af regler** mv., der skal efterleves
- Afklaring af **relevante særregler**
- **Internationale aspekter**
  - Er der grænseoverskridende aktiviteter – og hvordan håndterer I dem?

KROMANN
REUMERT

FASE 2
ANALYSE AF DATASTRØMME

SUNDKROGSGADE 5, DK-2100 KØBENHAVN Ø

CVR. NR: DK 62 60 67 11

KROMANN REUMERT

FASE 2 - ANALYSE AF DATASTRØMME (1)

Datastrømsanalysen skal danne grundlaget for compliance-arbejdet og kan anvendes til dokumentation iht. forordningen

› Hvilke data? Hvem anvender dataene? Til hvilke formål? Hvem har adgang? Videregives data? Mv.

Tilgang til analysen

› **Procesorienteret**

- Tager udgangspunkt i, hvordan data flyder i forbindelse med forretningens processer -> typisk ved interviews, workshops, beskrevne processer

› **Systemorienteret**

- Tager udgangspunkt i, hvilke IT-systemer virksomheden anvender, og hvorledes persondata lagres, anvendes og stilles til rådighed i disse

KROMANN REUMERT

FASE 2 - ANALYSE AF DATASTRØMME (2)

Dataindsamling

- **Interviews/workshops** med relevante interessenter
  - HR – IT - økonomi/finans - legal/compliance – ledelse/bestyrelse – salg – indkøb – eftermarked mv.
  - Husk grundig spørgeguide – og kritisk tilgang
- **Analyse af IT-systemer**
  - Hvilket indhold har systemerne? Almindelige og/eller følsomme oplysninger
  - Hvor er data placeret? Internt/eksternt/geografisk
  - Stemmer det overens med informationer indsamlet gennem interviews?
- *Husk også **eksterne parter og deres systemer** ift. jeres data flows*

Dokumentation

- Indsamling og gennemgang af **materiale** til fastlæggelse af datastrømme
- Udarbejdelse af en **illustrativ rapport** om datastrømme
  - Overblik til brug for compliance-analyse
  - Kan også efterfølgende bruges til at **dokumentere compliance** med persondataloven og persondataforordningen
- Sørg for, at dokumentationen er nem at opdatere
- **Verifikation** – få de interviewede m.v. til at gennemgå dokumentationen for at rette evt. fejl og misforståelser

KROMANN
REUMERT

FASE 3
COMPLIANCE-ANALYSE

SUNDKROGSGADE 5, DK-2100 KØBENHAVN Ø

KROMANN REUMERT

FASE 3 - COMPLIANCE-ANALYSE (1)

Formålet med compliance-analysen er at vurdere virksomhedens anvendelse af data i forhold til de relevante regler

- Afklaring af, hvilke oplysninger behandles til hvilke formål
- Vurdering af, om persondatabehandlingen er *lovlig* i forhold til persondataforordningens regler – og eventuelle andre relevante regelsæt
  - Grundlæggende en **gap-analyse,** der skal **identificere de gaps (huller), der skal lukkes, for at virksomheden efterlever gældende regler**

KROMANN REUMERT

FASE 3 - COMPLIANCE-ANALYSE (2)

1) **Grundlæggende behandlingsregler**

› Overholdelse af principperne om:

- Lovlighed, rimelighed og gennemsigtighed;
- **Formålsbegrænsning**;
- Dataminimering;
- Rigtighed (ajourføring);
- **Opbevaringsbegrænsning** (sletteplig);
- Integritet og fortrolighed;
- **Ansvarlighed** (accountability)

KROMANN REUMERT

FASE 3 - COMPLIANCE-ANALYSE (3)

2) **Behandlingshjemmel**

- Almindelige oplysninger
  - Samtykke? Kontrakt? Interesseafvejning?
- Følsomme oplysninger
  - Samtykke? Retskrav?
- Hvis *samtykkebaseret* behandling – er samtykket *gyldigt*?

3) **Håndtering af de registreredes rettigheder**

- Oplysningspligt
- Indsigtsret og ret til berigtigelse
- Håndtering af klager
- Kan virksomheden håndtere *ret til dataportabilitet* og *retten til at blive glemt*?
- Automatiske afgørelser, herunder profilering

KROMANN REUMERT

FASE 3 - COMPLIANCE-ANALYSE (4)

4) **Brug af databehandlere**

› **Overblik** over databehandleraftaler

› **Tilpasning** af aftalerne ift. forordningens krav om indholdet, herunder (i) *genstand for og varighed af behandlingen*, (ii) *behandlingens karakter og formål*, (iii) *typer af personoplysninger*, (iv) *kategorierne af registrerede*, og (v) *den dataansvarliges forpligtelser og rettigheder*

5) **Datasikkerhed**

› Gennemgang af **sikkerhedstiltag** - i dialog med IT

- F.eks. afsæt i sikkerhedskrav for anmeldte behandlinger hos Datatilsynet, ISO 2700x, branchestandarder mv.
- *Data protection by design* og *data protection by default*
- Konsekvensanalyse
- Risikobaseret tilgang – **med udgangspunkt i risiko for de registrerede**

KROMANN REUMERT

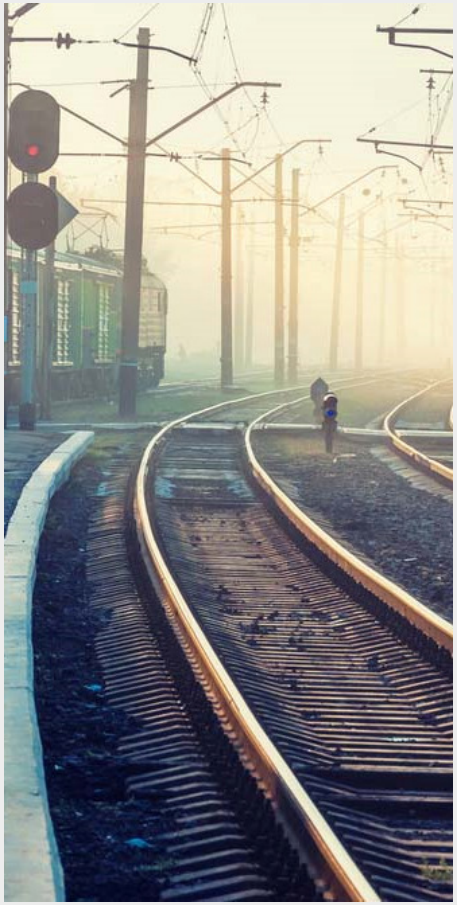
FASE 3 - COMPLIANCE-ANALYSE (5)

6) **Overførsler til udlandet**

- Inden for EU/EØS
- Uden for EU/EØS
  - Sikre tredjelande
  - EU Standardbestemmelser
  - Binding Corporate Rules
  - EU-US Privacy Shield
  - Ad hoc kontrakter
  - Evt. samtykke eller kontrakt
    - I visse tilfælde er en **forudgående** tilladelse fra Datatilsynet påkrævet

7) **Anmeldelse og tilladelse**

- Har virksomheden de fornødne tilladelser og anmeldelser hos Datatilsynet?



KROMANN REUMERT

FASE 3 - COMPLIANCE-ANALYSE (6)

Dokumentation

- Resultat af compliance-analysen – *gap-analyse*, der beskriver de områder, hvor virksomheden ikke lever op til reglerne
- Det endelige produkt: en **compliance-rapport** baseret på gap-analysen med angivelse af konkrete konklusioner og anbefalinger

KROMANN
REUMERT

FASE 4
HANDLINGSPLAN

SUNDKROGSGADE 5, DK-2100 KØBENHAVN Ø CVR. NR: DK 62 60 67 11

KROMANN REUMERT

FASE 4 - HANDLINGSPLAN (1)

Formålet med handlingsplanen er at fastlægge og prioritere de indsatser, der skal til for at udfylde hullerne fra gap-analysen – i rette tid og med rette prioritet

- Anbefalingerne fra compliance-rapporten danner grundlaget for udarbejdelse af en **handlingsplan**
- Handlingsplanen bør indeholde **anbefalinger og planer** for relevante tiltag
- Handlingsplanen bør indeholde **prioritering, deadlines og ansvarsfordeling**

KROMANN REUMERT

FASE 4 - HANDLINGSPLAN (2)

- Udarbejdelse af behandlingsoversigter og konsekvensanalyse (hvor relevant)

- Udarbejdelse af nye *politikker*, *guidelines, instrukser* mv. (eller tilpasning af de eksisterende)
  - *Eksempler: IT politik, politik/guidelines for håndtering af persondata/HR data/kundedata, instrukser for håndtering af klager, interne retningslinjer for whistleblowerordning, intern Code of Conduct, procedurer for tilfælde, hvor DPO/juridisk afdeling/IT skal involveres osv.*

- Træning af medarbejdere
  - Workshops, webinarer, krav om beståelse af en 'persondata test' mv.

- Udarbejdelse eller tilpasning af databehandleraftaler
  - *Procedurer* og/eller *tjeklister* til at sikre, at databehandleren er i stand til at give tilstrækkelige garantier for lovlig behandling
    - Revisorerklæringer, certificeringer mv.
  - Retningslinjer/procedurer for at indgå aftaler med databehandlere
  - Håndtering af eksisterende aftaler – ændring mv.

- Tilpasning af de øvrige dokumenter, såsom samtykketekster, privacy policies/notices, Binding Corporate Rules mv.

KROMANN REUMERT

FASE 4 - HANDLINGSPLAN (3)

- Tilpasning af IT systemer til at håndtere sletning, blokering, begrænsning, indsigtsret, de nødvendige sikkerhedstiltag mv.
  - Opfølgning hos tredjepartsleverandører
- Sikring af persondatabeskyttelse i igangværende udviklingsprojekter
  - *Data protection by design*
  - *Data protection by default*
- Indførelse af slettefrister mv.
- Implementering af procedurer til håndtering af sikkerhedsbrud, herunder konkrete instrukser til medarbejderne om:
  - Hvad der forstås ved et sikkerhedsbrud
  - Hvordan man skal agere mv.
- Procedurer for, hvordan man "boarder" en ny medarbejder/kunde mv. efter 25. maj 2018 for at sikre compliance
  - Nødvendig for enhver proces, hvor persondata er involveret
- Udarbejdelse af kontrolprocedurer og retningslinjer for håndtering af inspektioner/kontrolbesøg

KROMANN
REUMERT

FASE 5
IMPLEMENTERING

SUNDKROGSGADE 5, DK-2100 KØBENHAVN Ø

CVR. NR: DK 62 60 67 11

KROMANN REUMERT

FASE 5 - IMPLEMENTERING

Eksekvering af handlingsplanen

- Udarbejdelse af dokumenterne nævnt i handlingsplanen
  - Og der skal skabes kendskab til indholdet!
- Implementering af nye processer
- Uddannelse af medarbejdere
- Udpegning af en DPO, hvis lovkrav eller vurderes at være nødvendigt/hensigtsmæssigt
- Test af de tekniske løsninger og ændrede processer – de skal jo fungere den 25. maj 2018
- Evt. udeståender – hvis tidsplanen skrider
  - Hvordan og hvornår håndteres disse bedst?

VEDLIGEHOLDELSE

SUNDKROGSGADE 5, DK-2100 KØBENHAVN Ø

KROMANN REUMERT

VEDLIGEHOLDELSE

KROMANN REUMERT

KONTAKT

Tina Brøgger Sørensen
Partner

Direkte: +45 38 77 44 08
Mobil: +45 61 20 35 33
tib@kromannreumert.com