Erhvervsrådet i Høje-Taastrup
30. august 2017

Advokat Karina Bertelsen, CIPP/E, ADVODAN

PROGRAM

- Præsentation
- Del 1: General Data Protection Regulation (GDPR) / EU-forordningen
- Del 2: GDPR i praksis
- Del 3: Sådan kommer I videre

ADVODAN
– et netværk til forskel

PRÆSENTATION

KARINA LIND BERTELSEN
ERHVERVSADVOKAT /
PARTNER, CIPP-E certificering

ADVODAN GLOSTRUP

E-mail: kalb@advodan.dk
Telefon: 46 14 50 06

- Arbejder med persondata – både i forhold til kunder og intern compliance som advokat
- Medlem af Advodan-kædens fagudvalg for persondataret
- Medlem af JUC's netværk for persondataret
- Medlem af IAPP – verdens største forening for persondataspecialister – udbyder bl.a. certificeringen CIPP/E – (står for Certified Information Privacy Professional)

ADVODAN
– et netværk til forskel

PROGRAM – del 1 - reglerne

- Hvorfor regler om persondata?
- Grundlæggende principper for behandling af persondata
  - Hvad er persondata
  - Kategorier af persondata
  - Dataansvarlig ctr. Databehandler
  - God databehandlingsskik
  - Hjemmel til behandling
  - Behandlingssikkerhed
  - Den registreredes rettigheder

ADVODAN
– et netværk til forskel

HVORFOR OVERHOVEDET PERSONDATARET? - Historisk perspektiv

- Retten til privatliv er en grundlæggende menneskeret!
  - FNs resolution om grundlæggende menneskerettigheder fra 1948
- Persondataloven, som gennemførte EU-direktiv 95/46, trådte i kraft 1.7.2000
- Den generelle EU-forordning om persondata (GDPR), som blev vedtaget 14. april 2016, vil den 25. maj 2018 erstatte den danske persondatalov

ADVODAN
– et netværk til forskel

HVORFOR OVERHOVEDET PERSONDATARET? - Historisk perspektiv

- Der fremsættes i starten af folketingsåret 2017/18 forslag til ny person-datalov (”Databeskyttelsesloven”), som supplerer og udfylder GDPR på en række områder, f.eks.:
  - Samtykke fra børn
  - Personnumre
  - Strafbare forhold

- Meget vil være som i dag – men en række skærpelser

ADVODAN
– et netværk til forskel

HVAD ER PERSONDATA EFTER GDPR?

Definition: Enhver form for digital behandling af information om en identificeret eller identificerbar fysisk person (den registrerede)

Behandling skal forstås meget bredt. Den blotte registrering eller opbevaring af oplysninger er behandling, selv om oplysningerne ikke bruges

ADVODAN
– et netværk til forskel

HVAD ER PERSONDATA EFTER GDPR?

Eksempler på personoplysninger:

- Navn, adresse, mail, telefon, sociale forhold, familieforhold, helbredsforhold, indkomst- og formueforhold, lokationsdata, cpr-nummer, foto etc.

ADVODAN
– et netværk til forskel

HVAD ER IKKE PERSONDATA I GDPRs FORSTAND?

- Ikke oplysninger om juridiske personer (selskaber)
- Ikke afdøde personer (EU-forordningen)
  - Men DK lovudkast siger de er omfattet indtil 10 år efter død
- Ikke anonymiserede oplysninger
  - oplysninger, hvor det er umuligt at identificere personen bag
  - Pseudonymiserede data er omfattet
- Ikke rent manuel behandling (mundtligt formidlede oplysninger og håndskrevne noter), med mindre de indgår i et register
- GDPR gælder ikke for rent privat behandling (husholds-reglen)

ADVODAN
– et netværk til forskel

SÆRLIGE KATEGORIER AF PERSONDATA

- GDPR artikel 9 (følsomme oplysninger):
  - race eller etnisk oprindelse,
  - politisk, religiøs eller filosofisk overbevisning,
  - Fagforeningsmæssigt tilhørsforhold
  - Helbredsoplysninger
  - Seksuelle forhold og orientering
  - Genetiske og biometriske data (nyt)
- Strafbare forhold – GDPR artikel 10.
  - Oplysninger om straffedomme og lovovertrædelser, (afventer lovforslag)
- Personnumre – GDPR artikel 87 (afventer lovforslag)

ADVODAN
– et netværk til forskel

ØVRIGE PERSONDATA

- Alle personoplysninger, som ikke er omfattet af de særlige kategorier, er omfattet af reglerne for almindelige personoplysninger, men i praksis er der stor forskel på, hvordan de kan behandles.

- Jo mere fortrolige oplysninger, des mere skal der til for at kunne behandle dem (interesseafvejning), og jo større skal sikkerheden være.

ADVODAN
– et netværk til forskel

DATAANSVARLIG OG DATABEHANDLER

- Den dataansvarlige er den fysiske eller juridiske person, som afgør formål og midler for behandlingen
- En databehandler behandler persondata efter instruks fra en dataansvarlig - f.eks. et lønbureau eller rekrutteringsfirma
- Når den dataansvarlige overlader persondata til en databehandler, skal der laves en skriftlig databehandleraftale
- Pligterne overfor den registrerede (oplysning, indsigt etc.) påhviler den dataansvarlige.
- Kravene til behandlingssikkerhed gælder både for dataansvarlig og databehandler.

ADVODAN
– et netværk til forskel

GRUNDLÆGGENDE BEHANDLINGSPRINCIPPER

- Overhold god databehandlingsskik
- Persondata skal behandles lovligt, rimeligt og på gennemsigtig måde i forhold til den registrerede
- Persondata må ikke viderebehandles til andet formål end det, hvortil de er indsamlet (formålsbegrænsning)
- Data skal være tilstrækkelige, relevante og begrænset til det nødvendige for formålet (dataminimering)

ADVODAN
– et netværk til forskel

GRUNDLÆGGENDE BEHANDLINGSPRINCIPPER

- Data skal være korrekte og om nødvendigt ajourførte (rigtighed)
- Data må ikke opbevares i længere tid end nødvendigt (tidsbegrænsning)
- Data skal behandles på en måde, der giver tilstrækkelig sikkerhed mod uautoriseret brug, behandling, tilintetgørelse eller beskadigelse (datasikkerhed og fortrolighed)

ADVODAN
– et netværk til forskel

GRUNDLAG FOR BEHANDLING - ALMINDELIGE OPLYSNINGER

- **Samtykke fra den registrerede**
  - Samtykke skal være frit og oplyst, og kan altid trækkes tilbage
- Opfyldelse af en kontrakt som den registrerede er part i
- Retlig forpligtelse som påhviler den dataansvarlige iht. lov
- Beskyttelse af den registreredes vitale interesser (sundhed)
- Opgave i offentlig interesse/myndighedsudøvelse
- **Interesseafvejning; den dataansvarliges legitime interesser overfor den registreredes interesser**

ADVODAN
– et netværk til forskel

GRUNDLAG FOR BEHANDLING - SÆRLIGE KATEGORIER AF OPLYSNINGER

UDGANGSPUNKT: FORBUD MOD BEHANDLING, MED MINDRE:

- **Udtrykkeligt og specifikt samtykke**
- Opfyldelse af den dataansvarliges arbejds-, sundheds- og socialretlige forpligtelser
- Varetagelse af personens vitale interesser (liv eller død)
- Non-profit foreninger med særligt sigte (politisk, filosofisk, religiøst eller fagforeningsmæssigt)
- Oplysninger allerede offentliggjort af den registrerede
- Juridiske tvister
- Væsentlige samfundsinteresser
- Særlige undtagelser indenfor sundhed og forskning

ADVODAN
– et netværk til forskel

GRUNDLAG FOR BEHANDLING - SÆRLIGE KATEGORIER AF OPLYSNINGER

- **Strafbare forhold** (i henhold til høringsudkast til DK lov)
  - Private virksomheders behandling kræver samtykke fra den registrerede
  - Dog muligt at behandle uden samtykke, hvis det er nødvendigt til varetagelse af en berettiget interesse, og denne interesse klart overstiger hensynet til den registrerede

ADVODAN
– et netværk til forskel

GRUNDLAG FOR BEHANDLING - SÆRLIGE KATEGORIER AF OPLYSNINGER

- **Personnumre** kan behandles (efter høringsudkast til DK lov), når:
  - Det følger af lov
  - Den registrerede har givet samtykke
  - Af afgørende betydning for at sikre entydig identifikation
  - Når det kræves af en offentlig myndighed

- Offentliggørelse af personnummer kræver samtykke

ADVODAN
– et netværk til forskel

DEN REGISTREREDES RETTIGHEDER (DEN DATAANSVARLIGES PLIGTER)

- Oplysningspligt

- Ved indsamling hos den registrerede selv
- Ved indsamling hos tredjemand

- Indsigtsret
  - Pligt til efter anmodning fra den registrerede at give indsigt i oplysningerne om denne

ADVODAN
– et netværk til forskel

DEN REGISTREREDES RETTIGHEDER (DEN DATAANSVARLIGES PLIGTER)

- Indsigelsesret
  - Stoppe behandling/slette, hvis indsigelsen er berettiget
- Berigtigelse af forkerte/forældede oplysninger
- Sletning af oplysninger, hvor grundlaget for behandling er væk

ADVODAN
– et netværk til forskel

OVERVEJELSER VED INDSAMLING OG BEHANDLING AF PERSONOPLYSNINGER

- Er der et saglig formål med behandlingen?
  - Skal vurderes ved både enhver indsamling, brug, videregivelse
- Er der hjemmel til at behandle oplysningen – hvilken?
- Hvem skal have adgang til oplysningen?
- Hvordan skal oplysningerne overføres til relevante personer?
- Hvor længe skal de gemmes? – sletning?
- Må oplysningen bruges til andre formål? (samtykke)
- Er der tilstrækkelig behandlingssikkerhed?
- Hvordan opfyldes oplysningspligten?

ADVODAN
– et netværk til forskel

OPLYSNINGSPLIGTENS OMFANG

- Identitet og kontaktoplysninger på den dataansvarlige + evt. DPO
- Formålene med behandlingen og grundlaget herfor
- Hvilke oplysninger indhentes og fra hvem
- Eventuelle modtagere af oplysningerne, herunder i tredjelande
- Hvor længe oplysninger opbevares (slettefrist)
- Retten indsigt og sletning mv.
- Retten til at trække et samtykke tilbage samt konsekvenser heraf
- Retten til at klage til Datatilsynet

ADVODAN
– et netværk til forskel

OPLYSNINGSPLIGTEN
- begrænsninger og frister

- Ikke pligt til at give oplysninger, som allerede er den registrerede bekendt
- Ikke pligt til at give oplysninger, hvis det strider mod tavshedspligt

Frister:

- Uden unødigt ophold, normalt max. 1 måned.
- Hvis indsamling med henblik på videregivelse – inden videregivelse

ADVODAN
– et netværk til forskel

HVAD ÆNDRER EU-FORORDNINGEN?
- De vigtigste nyskabelser

- Forøgede **rettigheder for de registrerede**
  - Øget oplysningspligt for den dataansvarlige (f.eks. slettefrist)
  - Ret til at blive glemt (også ift. tredjemand)
  - Ret til at få egne data i maskinlæsbart format (f.eks. USB)
  - Den dataansvarlige skal aktivt bistå den registrerede med at udnytte sine rettigheder – f.eks. vha. Klagevejledning
  - Indsigelsesret mod ”profilering”

ADVODAN
– et netværk til forskel

HVAD ÆNDRER EU-FORORDNINGEN? - De vigtigste nyskabelser - 2

- Forøgede **pligter for den dataansvarlige**
  - Dokumentation for de behandlinger, der foretages, slettefrister, sikkerhedsforanstaltninger mv.
  - Pligt til at udarbejde konsekvensanalyser – efter risikovurdering (systematisk behandling eller overvågning)
  - Pligt til selvanmeldelse til Datatilsynet ved databrud (inden 72 timer) – f.eks. hackerangreb
  - Pligt til underretning af den/de registrerede om brud, der medfører risiko for den registrerede

ADVODAN
– et netværk til forskel

HVAD ÆNDRER EU-FORORDNINGEN? - De vigtigste nyskabelser - 3

- Forøgede **pligter for databehandlere**
  - Selvstændigt ansvarlig overfor de registrerede
  - Skal bistå den dataansvarlige med at overholde sine forpligtelser

ADVODAN
– et netværk til forskel

HVAD ÆNDRER EU-FORORDNINGEN? - De vigtigste nyskabelser - 4

Databeskyttelsesrådgiver (DPO) udpeges (intern eller ekstern)

- Ved behandling af følsomme oplysninger i større omfang eller brug af overvågning

Databeskyttelse gennem design af it-systemer og standardindstillinger

- F.eks. Intern adgangskontrol til IT-systemer

ADVODAN
– et netværk til forskel

HVAD ÆNDRER EU-FORORDNINGEN? - De vigtigste nyskabelser - 5

Betydelige sanktioner:

- Store bøder (grove overtrædelser)
  - Op til 4 % af virksomhedens globale omsætning eller EUR 20 mio. (hvad der er højest)

- ”Små” bøder (mindre grove overtrædelser)
  - Op til 2 % af virksomhedens globale omsætning eller EUR 10 mio. (hvad der er højest)

ADVODAN
– et netværk til forskel

DEL 2: GDPR I PRAKSIS

PROGRAM del 2 – GDPR i praksis
- fokusområder for alle virksomheder

- IT-sikkerhed
- Kundeoplysninger
- Hjemmeside / markedsføring
- Medarbejderoplysninger
- Databehandleraftaler med leverandøren
- Virksomheden som databehandler
- Fortegnelse (intern dokumentation)
- Udpege persondataansvarlig (evt. DPO)

ADVODAN
– et netværk til forskel

IT-SIKKERHED

- Ingen IT-systemer er 100% sikre. Risikobaseret tilgang.
  - Sikkerhedsniveau skal afspejle risici (jo større risici, jo større krav)
  - Vælge løsninger og handlinger, som begrænser konkrete risici
  - Tilstrækkeligt sikkerhedsniveau (hensyn til bl.a. den teknologiske udvikling, omkostninger, risiko ved brud m.v.)
- IT-sikkerhedspolitik, herunder forholdsregler ved databrud, adgangskontrol i sagssystemer, instrukser og regler for struktureret lagring og sletning af data (bør drøftes med IT-leverandør)

ADVODAN
– et netværk til forskel

IT-SIKKERHED
PRAKTISKE RÅD

- Automatisk aflogning på PC efter f.eks. 5 minutter
- Skift passwords regelmæssigt, f.eks. hver 3. måned
- Benyt passwords, der ikke let kan ”knækkes”
- Brug forskellige passwords til hhv. login på pc og sagssystem
- Sørg for, at bærbare enheder (labtops, iphone og ipads etc.) er beskyttet med password og at indholdet er krypteret
- Beskyt sagsmapper, der indeholder følsomme oplysninger
- Brug sikker print funktion ved følsomme oplysninger

ADVODAN
– et netværk til forskel

SÆRLIGT OM E-MAILS

- Send ikke følsomme/fortrolige oplysninger på en ukrypteret e-mail. Benyt signaturløsningen eller e-boks
- Det samme gælder personnumre og andre fortrolige oplysninger , f.eks. privatøkonomi
- Hvis der sendes ekstern mail til flere end nogle få modtagere (som kender hindanden), så skal Bcc-feltet benyttes, så adresserne ikke er synlige for modtagerne.

ADVODAN
– et netværk til forskel

CRM / KUNDEDATABASE

- Indsamling af kontaktoplysninger på kunder
- Indsamling af almindelige (kontakt)oplysninger kan ske ud fra en interesseafvejning – dog næppe adressebeskyttede
- Oplysningerne må ikke anvendes til direct marketing / nyhedsbreve uden samtykke
- Man skal sikre sig, at oplysningerne holdes ajour
- Man skal opfylde oplysningspligten senest ved første kontakt
- Undlad registrering af private oplysninger, herunder helbredsforhold, familiesituation m.v.

ADVODAN
– et netværk til forskel

HJEMMESIDE / MARKEDSFØRING

- Cookiepolitik på hjemmesiden
- Persondatapolitik
- Tilmelding til nyhedsbreve
- Rekruttering (oplysningspligt overfor jobansøgere)

ADVODAN
– et netværk til forskel

MEDARBEJDEROPLYSNINGER

- Virksomheden er dataansvarlig
- Intern persondatapolitik til alle medarbejdere
- Overvågning af medarbejdere (e-mail, GPS, mobil)
- Specifikke instrukser til HR- og lønmedarbejdere
- Uddannelse af alle medarbejdere
- Håndtering af persondata ved rekruttering
- Håndtering af persondata under ansættelsen
- Håndtering af persondata ved fratræden

ADVODAN
– et netværk til forskel

MEDARBEJDEROPLYSNINGER
Opbevaring af oplysninger

- Oplysninger om ansøgere:
  - Kun relevante ansøgninger bør gemmes
  - Krav om samtykke
  - Max 6 måneder

- Oplysninger om medarbejdere:
  - Oplysninger afgivet af medarbejderen må opbevares uden specifikt samtykke
  - Visse oplysninger bør slettes straks efter ansættelse (ex. straffeattester og lign.)

ADVODAN
– et netværk til forskel

MEDARBEJDEROPLYSNINGER
Opbevaring af oplysninger

- Periode for opbevaring af medarbejderoplysninger:
  - Virksomheder bør have procedurer for opbevaring / sletning af medarbejderoplysninger
  - Oplysninger skal slettes, når de ikke længere er relevante. Vurderes individuelt
  - Situationer hvor det kan være sagligt at gemme relevante oplysninger i længere tid:
    - Opsigelsessager
    - Tvistsager
    - Arbejdsskade
  - Dokumentationskrav / bogføringsloven m.v.

ADVODAN
– et netværk til forskel

MEDARBEJDEROPLYSNINGER
Medarbejderoplysninger på internettet

- Medarbejderoplysninger på internettet
  - Arbejdsrelaterede oplysninger (navn, arbejdsområde, ansættelsesår, arbejdstelefon, e-mail) kan som udgangspunkt offentliggøres uden samtykke
  - Oplysninger af privat karakter (ex. billede, privat adresse, privat e-mail, privat telefonnummer) kræver udtrykkeligt samtykke
  - En medarbejder har mulighed for at gøre indsigelse overfor offentliggørelse

ADVODAN
– et netværk til forskel

MEDARBEJDEROPLYSNINGER
Kontrolforanstaltninger

- Kontrol af medarbejdere (ex. logning og kontrol af e-mails, tjek af GPS m.v.)
  - Medarbejdere skal kende procedurer i forvejen
  - Skal være nødvendigt for at forfølge berettiget interesse (ex. kontrol- eller sikkerhedshensyn)
  - Private e-mails må ikke læses

ADVODAN
– et netværk til forskel

MEDARBEJDEROPLYSNINGER
Sikkerhedsprocedurer

- Krav om sikkerhedsprocedurer:
  - Adgang til personoplysninger skal begrænses – både ved instrukser og IT-redskaber
  - Retningslinjer for brug af hjemmearbejdspladser og mobile devices, hvorfra der er adgang til personoplysninger
  - Adgang til fratrådte medarbejderes e-mail konto skal begrænses

ADVODAN
– et netværk til forskel

DATABEHANDLERAFTALER MED LEVERANDØRER

- Virksomheder er ansvarlige for at indgå databehandleraftaler med leverandører (ex. lønsystemer, cloud-løsninger, HR-løsninger m.v.)
- Virksomheden skal være kritisk og stille krav til særligt databehandlerens IT-sikkerhed
- Særlig opmærksom på beliggenhed i EU
- Brug af underdatabehandlere

ADVODAN
– et netværk til forskel

DATABEHANDLERAFTALER – NEED TO HAVE

- Instruks
- Autoriseret personale
- Tilvejebringes information til brug for risikovurderinger / sikkerhedstiltag
- Bistand til at opfylde dataansvarliges pligt til at hjælpe
- Dokumentation ved databrud
- Audits fra den dataansvarlige
- Cloud løsninger / underdatabehandlere
- Aftalens ophør
- Sletning af data ved ophør
- Bestemmelser ved brud

ADVODAN
– et netværk til forskel

VIRKSOMHEDEN SOM DATABEHANDLER

- Virksomheder, der behandler persondata på vegne af kunder, er databehandlere
- GDPR indfører selvstændigt ansvar for databehandlere
- Pligt til at bistå den dataansvarlige (kunden)
- Brug af underdatabehandlere

ADVODAN
– et netværk til forskel

FORTEGNELSE OVER BEHANDLINGSAKTIVITETER (ART. 30)

- Intern dokumentation, som skal stilles til rådighed for Datatilsynet efter anmodning
- Forpligtelsen omfatter både dataansvarlige og databehandlere
- Som udgangspunkt alene en forpligtelse med over 250 medarbejdere, medmindre der regelmæssigt behandles særlige kategorier af oplysninger eller behandlingen på anden måde kan medføre risiko for de registrerede
- Anbefaling at der altid udarbejdes en fortegnelse

ADVODAN
– et netværk til forskel

UDPEGE ANSVARLIG FOR PERSONDATA

- Udpege en intern ansvarlig for virksomhedens persondata compliance
- Håndtere henvendelser fra registrerede
- Håndtere kommunikation med Datatilsynet, herunder ved brud på datasikkerheden
- Gennemgå databehandleraftaler
- Ajourføring af politikker og instrukser
- Uddannelse af medarbejdere

ADVODAN
– et netværk til forskel

DATABESKYTTELSESRÅDGIVER (DPO)

- Hvis kerneaktiviteten består i behandling af særlige kategorier af oplysninger, herunder vedrørende helbredsforhold, og der er tale om en behandling i stort omfang, skal virksomheden udpege en DPO (intern eller ekstern)
- DPO kan være en ansat eller en ekstern – krav om *"faglige kvalifikationer, navnlig ekspertise inden for databeskyttelsesret og – praksis samt evne til at udføre nævnte opgaver*"
- Kendskab til lovgivning, både nationalt og GDPR
- "Evne til at udføre opgaver": Vedrører både faglig viden og personlige kompetencer / ansvarsområder

ADVODAN
– et netværk til forskel

DATABESKYTTELSESRÅDGIVER (DPO)

- DPO'ens opgaver:
  - Information og rådgivning til den data-ansvarlige (uddanne medarbejdere m.v.)
  - Overvåge compliance
  - Gennemføre konsekvensanalyser
  - Samarbejde med Datatilsynet
  - Kontaktperson for Datatilsynet

ADVODAN
– et netværk til forskel

DATABESKYTTELSESRÅDGIVER (DPO)

- Krav til data-ansvarlig / databehandler:
  - Skal inddrage DPO'en tilstrækkeligt og rettidigt
  - Skal støtte DPO'en (herunder ved at sikre fornødne ressourcer)
  - Må ikke give instrukser til DPO
  - Må ikke afskedige eller straffe DPO som følge af dennes udøvelse af rollen som DPO

ADVODAN
– et netværk til forskel

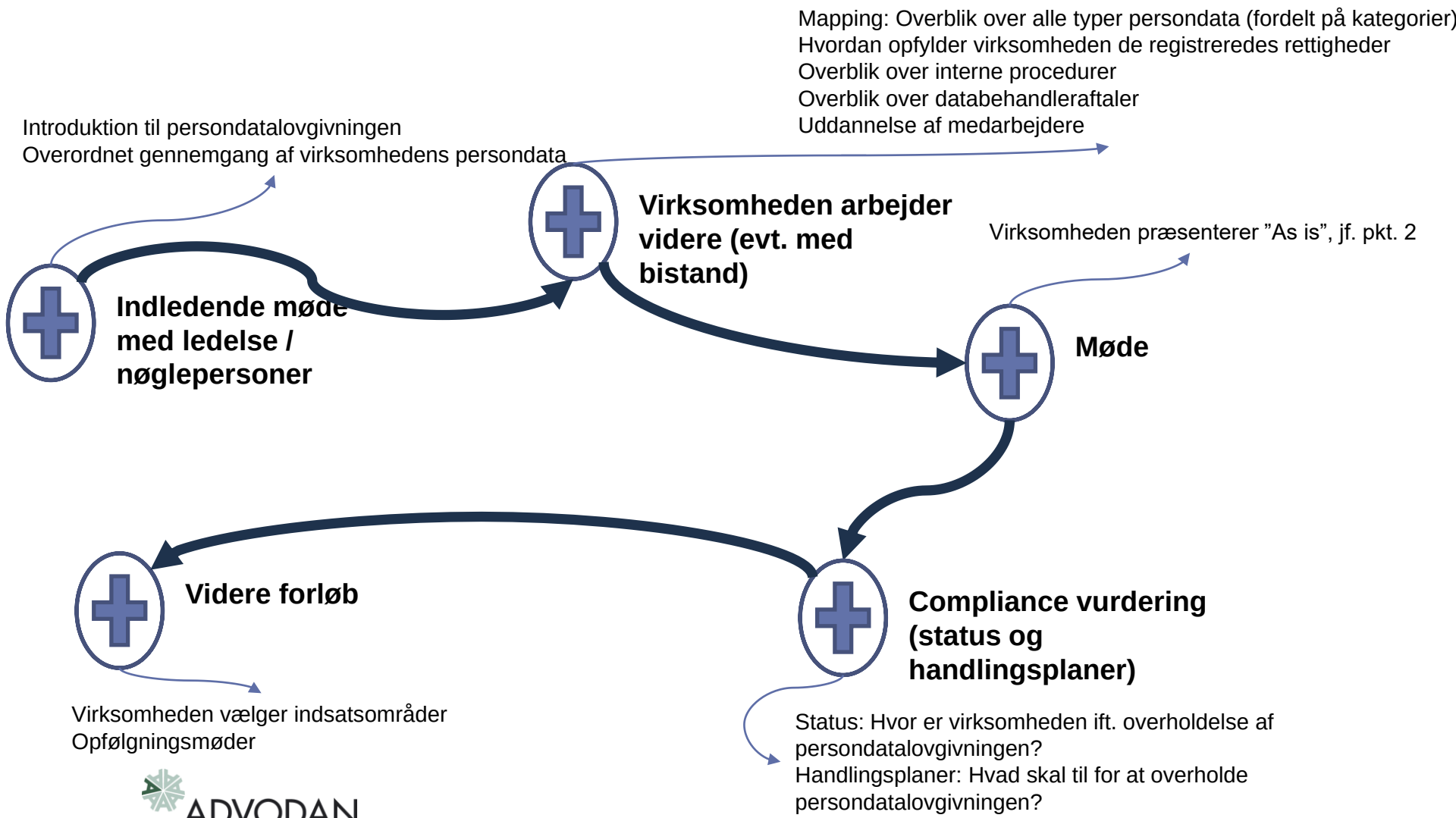
DEL 3: SÅDAN KOMMER I VIDERE…

COMPLIANCE

- Management!
- IT & Jura – fokus på begge dele
- Skab overblik over alle persondata i virksomheden
- Identificér indsatsområder

ADVODAN
– et netværk til forskel

JURATJEK



ADVODAN
– et netværk til forskel

AFSLUTNING

SPØRGSMÅL…

ADVODAN
– et netværk til forskel