PERSONDATA

- GDPR I PRAKSIS

Karina Lind Bertelsen, advokat / partner
CIPP/E, CIPM
kalb@advodan.dk / 46 14 50 06

ADVODAN

AGENDA – SUPEROFFICE DEN 7. FEBRUAR 2018

- Hvor langt er virksomhederne med GDPR?
- GDPR i overblik – med praktiske eksempler
- Hvordan kommer man som virksomhed i mål?

ADVODAN

HVOR LANGT ER VIRKSOMHEDERNE?

- Erfaringer med mindre og mellemstore virksomheder:
  - Erkendelsen vokser
  - Manglende fokus fra ledelsen
  - Mange misforståelser
  - Svært ved at få overblik over opgaverne –> mange går i stå
- Nødvendigt at den eller de ansvarlige kender reglerne og har en plan…
- Mange har travlt!

ADVODAN

DET HANDLER OM MENNESKERETTIGHEDER!

- Retten til privatliv er en grundlæggende menneskeret!
- Den enkelte person (den registrerede) skal have viden om og kontrol med, hvad deres personlige oplysninger bruges til.
- Siden 1. juli 2000 har persondataloven været gældende – men få kender til den, og endnu færre overholder den. Den er baseret på et EU-direktiv fra 1995.
- Når GDPR træder i kraft den 25. maj 2018, vil ca. 80 % være regler, der allerede gælder i dag.
- Noget af det nye er øgede dokumentationskrav
- GDPR suppleres af andre regler, bl.a. en dansk databeskyttelseslov (ej vedtaget endnu) og en E-databeskyttelsesforordning (forhandles p.t. i EU-parlamentet).

ADVODAN

HVAD ER PERSONDATA?

Definition af "Personoplysninger", jf. art. 4, nr. 1:

"Enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede)…"

De i praksis vigtigste grupper af personer:

- Medarbejdere
- Kunder (særligt B2C, men også B2B)
- Samarbejdspartnere

Eksempler:

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

Pseudonymiserede data er omfattet.

Eksempel brug af stregkoder, medarbejdernummer i stedet for navn osv.

Anonymiserede oplysninger er ikke omfattet. Forudsætter, at det på ingen måde er muligt at knytte til en person.

ADVODAN

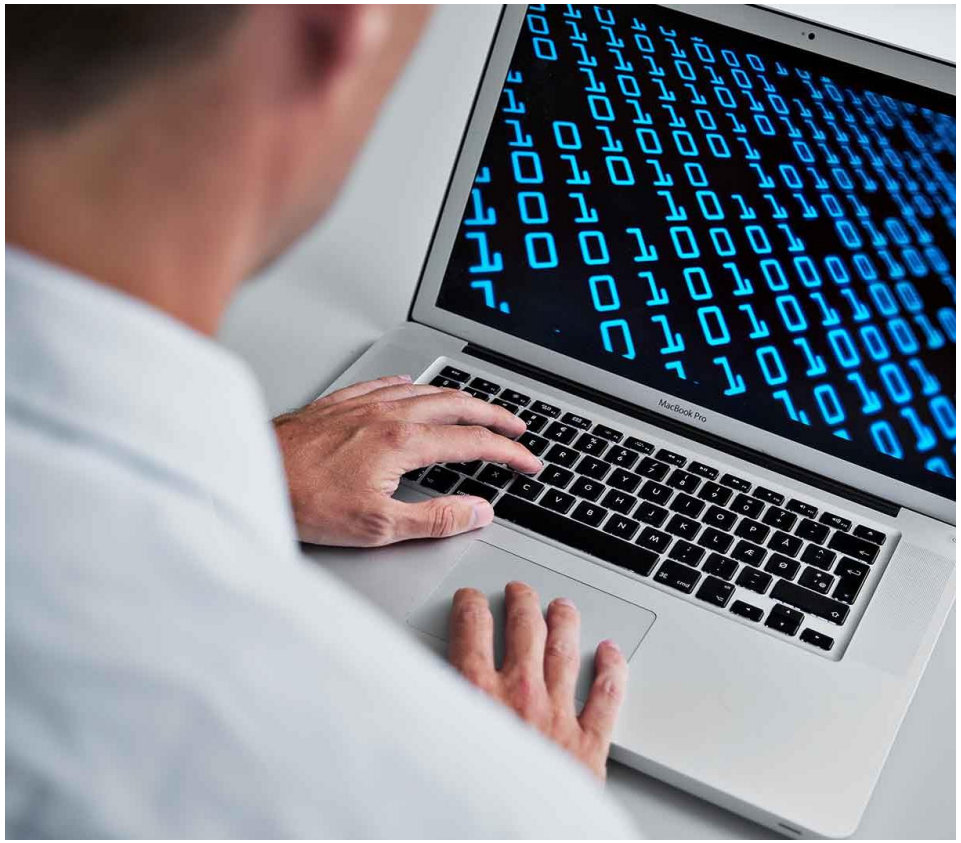
HVORNÅR ER VI INDENFOR GDPR?

Når der foretages en **elektronisk behandling**

Behandling skal forstås bredt og omfatter alt fra indsamling, videregivelse, brug, opbevaring, sletning osv.

Undtagelser:

- Rent manuel behandling (mundtligt formidlede oplysninger og håndskrevne noter), med mindre de indgår i et register
- Privat behandling (husholdsreglen)
- Oplysninger om juridiske selskaber



ADVODAN

PERSONDATA ER IKKE BARE PERSONDATA - FORSKELLIGE KATEGORIER

Særlige kategorier (GDPR art. 9) – mest følsomme

- Race, etnisk oprindelse, politisk, religiøs el. filosofisk overbevisning, fagforeningsmæssige tilhørsforhold, genetiske data, biometriske data mhp. entydig identifikation, helbredsoplysninger, seksuelle forhold eller orientering

Andre særlige typer oplysninger:

- Straffedomme og lovovertrædelser
- CPR-numre

De "almindelige" persondata – GDPR art. 6

- Væsentlige sociale problemer, andre rent private forhold, økonomi, skat, gæld, sygedage, tjenstlige forhold, familieforhold, bolig, bil, eksamen, ansøgning, CV, ansættelsesdato, stilling, arbejdsområde, arbejdstelefon, navn, adresse, fødselsdato.

- Selv om de er "almindelige", kan de godt være private og fortrolige!

ADVODAN

TO ROLLER
- AFGØRENDE FORSKELLE

Dataansvarlig

- Typisk en virksomhed, offentlige myndighed eller andet organ, der – alene eller sammen med andre – afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger.

Eksempler:

- En arbejdsgiver dataansvarlig for oplysninger om sine ansatte
- En virksomhed er ansvarlig for oplysningerne i sit kundekartotek/CRM-system

Databehandler

- Typisk en virksomhed, der behandler personoplysninger på den dataansvarliges vegne og efter instruks fra den dataansvarlige.

Eksempler:

- En hosting-virksomhed, der hoster kundevirksomheders data, er databehandler
- Det samme er Bluegarden, når de laver løn for deres kunder

ADVODAN

ALMINDELIGE OPLYSNINGER - BEHANDLINGSGRUNDLAG

- **Samtykke** fra den registrerede

- **Opfyldelse af en kontrakt** som den registrerede er part i
  - F.eks. adresse til levering af varer købt online
  - F.eks. oplysninger afgivet af den registrerede selv til brug for en erhvervsdrivendes afgivelse af tilbud

- **Retlig forpligtelse** som påhviler den dataansvarlige
  - F.eks. lønoplysninger til SKAT
  - Krav om udtrykkelig forpligtelse uden element af frivillighed for den dataansvarlige

- Et samtykke er en **frivillig, specifik, informeret og utvetydig** viljetilkendegivelse.
- Oplysningspligt skal opfyldes
- Hvis samtykke indgår i en skriftlig erklæring med andre forhold, skal samtykke tydeligt kunne skelnes fra de øvrige forhold, i lettilgængeligt sprog
- Der skal oplyses om muligheden for at trække samtykke tilbage
- Den dataansvarlige har bevisbyrden for, at samtykke er givet

ADVODAN

ALMINDELIGE OPLYSNINGER - BEHANDLINGSGRUNDLAG

- Beskyttelse af den registreredes vitale interesser (sundhed)
- Opgave i offentlig interesse/myndighedsudøvelse
- **Interesseafvejning; den dataansvarliges legitime interesser overfor den registreredes interesser**
  - F.eks. Logning af internetbrug, almindelig kundedatabase, videregivelse indenfor koncern

- Interesseafvejningsreglen er i praksis et hyppigt anvendt behandlingsgrundlag, men husk at den ikke kan bruges ved følsomme oplysninger

ADVODAN

FØLSOMME OPLYSNINGER - BEHANDLINGSGRUNDLAG

UDGANGSPUNKT: FORBUD MOD BEHANDLING, MED MINDRE:

- **Udtrykkeligt og specifikt samtykke**
- Opfyldelse af den dataansvarliges arbejds-, sundheds- og socialretlige pligter - se databeskyttelseslov § 12
- 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

- Husk at samtykke til at behandle personoplysninger ikke uden videre omfatter personens følsomme oplysninger.
- Hav særlig fokus på sletning af følsomme oplysninger
- Vær opmærksom på, at kommunikation indeholdende følsomme oplysninger bør sikres med kryptering

ADVODAN

PERSONNUMRE - BEHANDLINGSGRUNDLAG

- **Personnumre** kan behandles, 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

- Vær opmærksom på risikoen for, at et CPR-nummer i de forkerte hænder kan misbruges til identitetstyveri
- Lad være med at skrive CPR-numre i kontrakter, medarbejderlister mv.
- Benyt kryptering, hvis mails eller vedhæftede filer indeholder CPR-numre

ADVODAN

PRINCIPPERNE LOVLIGHED, RIMELIGHED OG GENNEMSIGTIGHED

- **Lovlighed**: Man skal overholde gældende lovgivning, både regler i GDPR og udenfor denne
- **Rimelighed** betyder bl.a., at der skal være et sagligt formål med behandlingen / krav om proportionalitet
- **Gennemsigtighed** overfor de registrerede
  - Man skal vide, hvilke oplysninger, der behandles om en, til hvilke formål og af hvem

Det betyder bl.a.:

- At der skal være et lovligt **grundlag** for behandling
- At du skal holde virksomhedens interesse i behandlingen op imod den registreredes interesse i at beskytte sine private oplysninger
- At du skal sørge for, at virksomheden opfylder sin oplysningspligt ved enhver behandling af persondata

ADVODAN

PRINCIPPERNE FORMÅLSBEGRÆNSNING, DATAMINIMERING OG RIGTIGHED

Formålsbegrænsning betyder, at du kun må behandle persondata til det formål, de er indsamlet

- Vil du bruge dem til andet, må du først spørge om lov

Dataminimering betyder, at du ikke skal indsamle flere oplysninger end nødvendigt

Rigtighed indebærer, at du ikke (bevidst) må behandle forkerte data. Du skal rette data, hvis du bliver opmærksom på fejl

En arbejdsgiver må f.eks. Ikke sende personaleoplysninger til en samarbejds-partner, så denne kan markedsføre produkter overfor de ansatte

Lad være med at indsamle private oplysninger om dine forretnings-forbindelser

Giv de registrerede mulighed for at gøre opmærksom på ændringer

ADVODAN

OPBEVARINGSBEGRÆNSNING

Man må ikke gemme personoplysninger længere end det er nødvendigt.

- Fristen for at slette oplysningerne afhænger af det konkrete forhold.
- Hvor længe skal du gemme for at opfylde lovgivning (f.eks. bogføringsloven)
- Hvor længe rækker virksomhedens berettigede interesse i at gemme?
- Der skal tages stilling inden indsamlingen!

Eksempler:

- Datatilsynet har udtalt, at jobansøgninger og CV'er maksimalt må gemmes 6 måneder.
- Oplysninger om fratrådte medarbejdere må højst gemmes 5 år efter fratrædelse.
- Oplysning om kundeforhold må gemmes til udløb af reklamationsfrist etc.

ADVODAN

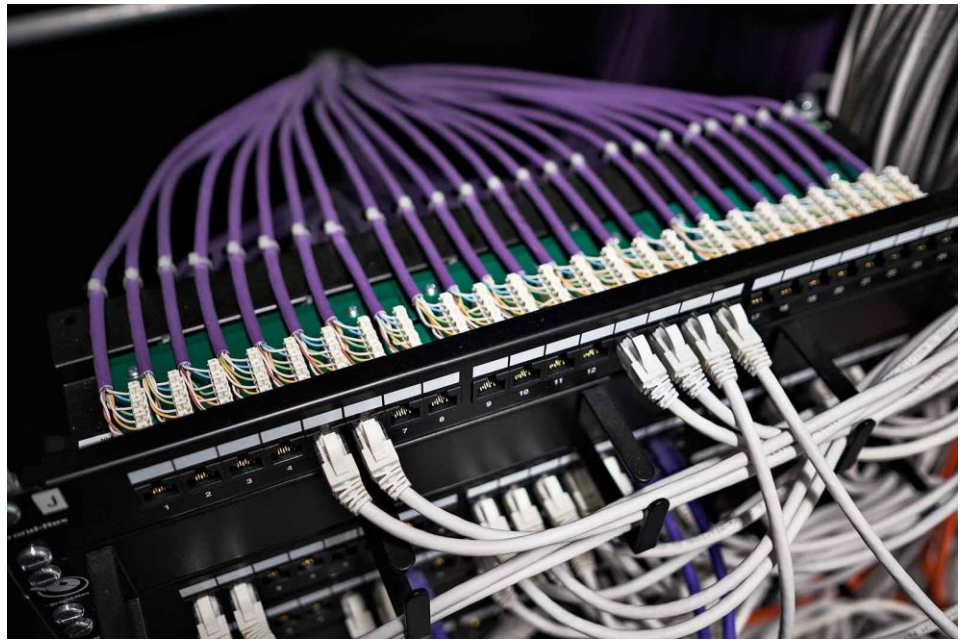
INTEGRITET OG FORTROLIGHED

Uvedkommende skal ikke have adgang til personoplysninger!

Det handler dels om IT-sikkerhed i hardware og software

Men det handler i lige så stor grad om mennesker:

- Procedurer for adgangsbegrænsning
- Procedurer for indsamling og journalisering
- Datadisciplin



ADVODAN

ANSVARLIGHED

- Den dataansvarlige skal kunne **dokumentere**, at man lever op til de grundlæggende principper
- Stiller krav om skriftlige politikker, procedurer og instrukser for den daglige omgang med persondata
- Fortegnelser over behandlingsaktiviteter
- Procedurer for de særlige situationer
  - Anmodninger fra de registrerede (indsigt, sletning etc.)
  - Håndtering af databrud

ADVODAN

DE REGISTREREDES RETTIGHEDER, F.EKS. OPLYSNINGSPLIGT

- Oplysningspligten gælder både ved indsamling hos den registrerede og hos tredjemand.
- Skal gives i et klart og letforståeligt sprog
- Skal gives uden unødig forsinkelse og **senest:**
  - En måned efter indsamlingen
  - Inden videregivelse
  - Ved første kontakt, hvis der er tale om kontaktoplysninger på den registrerede
- Undtagelser
  - Hvis det strider mod lovbestemt tavshedspligt
  - Hvis oplysningerne allerede er givet
  - Hvis det er umuligt eller uforholdsmæssigt tidskrævende (snæver undtagelse)

- 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
- Retten indsigt og sletning mv.
- Retten til at trække et samtykke tilbage samt konsekvenser heraf
- Retten til at klage til Datatilsynet

ADVODAN

ANDRE RETTIGHEDER

- Indsigtsret
- Ret til sletning
- Ret til indsigelse
- Ret til berigtigelse af oplysninger
- Ret til dataportabilitet

- OBS – der kan være undtagelser, hvorfor begæringer ikke nødvendigvis skal efterleves…
- Vigtigt at have styr på, hvornår man skal efterleve en begæring

ADVODAN

DEN DATAANSVARLIGE SKAL:

- Være i stand til at **påvise**, at man overholder reglerne. Dette forudsætter
  - Skriftlige databeskyttelsespolitikker
  - Passende **tekniske** og **organisatoriske** foranstaltninger
- Udarbejde **fortegnelser over behandlingsaktiviteter** (nyt dokumentationskrav)
- Sørge for at benytte IT-systemer mv., der opfylder kravet om ”Privacy by Design”
- Sikre procedurer vedrørende anmeldelse af databrud til Datatilsynet (indenfor 72 timer)

Eksempler på dokumentation:

- IT-sikkerhedspolitik
- Interne instrukser for håndtering af medarbejder- og kundedata
- Afsnit (oplysning) i medarbejderhåndbog om behandling af medarbejderdata
- Oplysning på hjemmeside om behandling af kundedata, cookies mv.
- Oplysning i aftalebreve, ordrebekræftelser mv.
- Instrukser om håndtering af databrud, indsigtsanmodninger mv.

ADVODAN

BRUG AF DATABEHANDLERE

- Virksomheder er ansvarlige for at indgå databehandleraftaler med leverandører (ex. lønsystemer, cloud-løsninger, HR-løsninger m.v.)
- Begge parter har et ansvar for at sikre, at aftalen indgås
- Virksomheden skal være kritisk og stille krav til særligt databehandlerens IT-sikkerhed
- Særlig opmærksom på beliggenhed i EU / EØS
  - Kræver en helt særlig aftale at føre data ud af EU
- Brug af underdatabehandlere kræver godkendelse af dataansvarlig

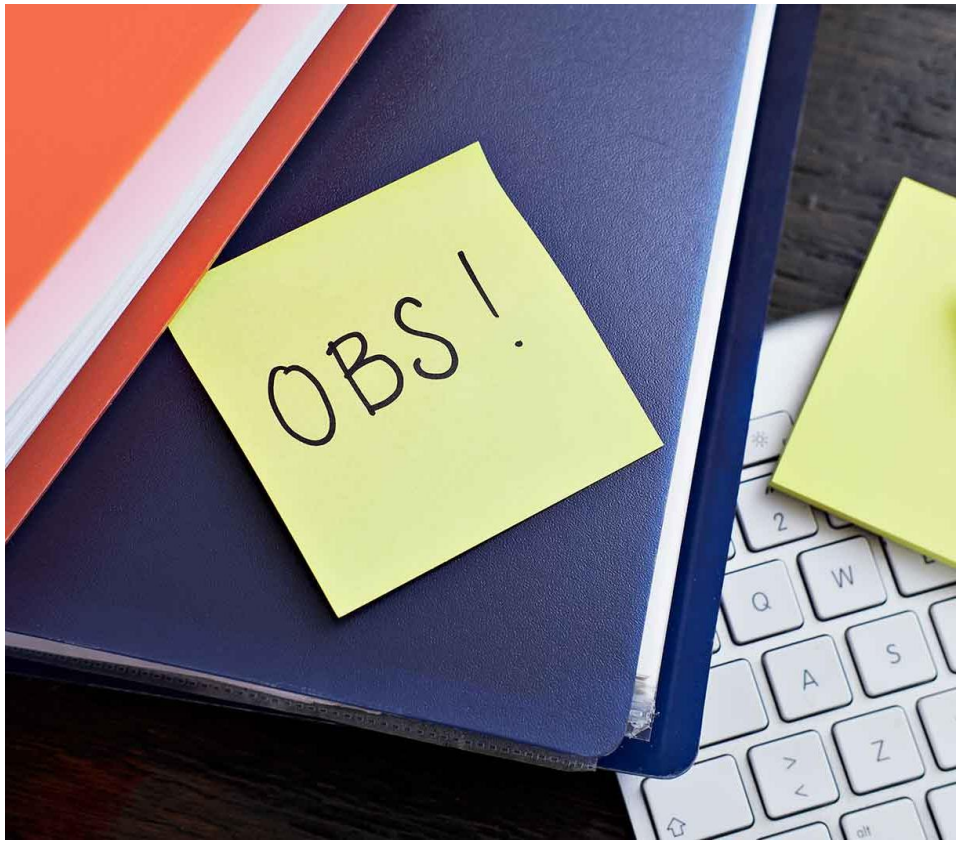
Indhold af databehandleraftalen

- Instruks fra den dataansvarlige
- Tavshedspligt/fortrolighed
- Oplysning om tekniske og organisatoriske sikkerhedsforanstaltninger hos databehandler
- Forbud mod underdatabehandler (herunder hosting) uden samtykke
- Bistand til besvarelse af datasubjekters anmodninger
- Dokumentation ved databrud
- Audits fra den dataansvarlige
- Sletning eller tilbagelevering af data ved aftalens ophør

ADVODAN

TILSYN OG SANKTIONER

- Tilsynsbesøg fra Datatilsynet uden retskendelse
- Datatilsynet får beføjelse til at udstede administrative bøder (bødeforlæg).
- Datatilsynet kan nedlægge påstand om rettighedsfrakendelse for visse brancher
- Bøder – 2 niveauer
  - Op til 4 % af omsætning eller 20 mio. EUR for ”materielle” overtrædelser – behandling i strid med grundlæggende regler
  - Op til 2 % af omsætning eller 10 mio. EUR for ”formelle” overtrædelser - manglende dokumentation etc.
- Erstatning og offentliggørelse



ADVODAN

HVEM SKAL I PRAKSIS STÅ FOR DET?

Alle bør udpege en internt ansvarlig for persondata til at

- Håndtere henvendelser fra registrerede
- Håndtere kommunikation med Datatilsynet, herunder ved brud på datasikkerheden
- Gennemgå databehandleraftaler
- Ajourføre politikker og instrukser
- Uddanne medarbejdere

Nogle virksomheder skal have en **databeskyttelsesrådgiver (DPO)**, hvis man:

- Som en del af virksomhedens **kerneforretning** enten
  - Behandler **følsomme oplysninger** eller
  - Beskæftiger sig med **systematisk overvågning** af personer
- Og forudsat at denne aktivitet har et **større omfang**

DPO'en kan være ekstern (konsulent)

ADVODAN

HVORDAN KOMMER MAN SOM VIRKSOMHED I MÅL?

- Udpeg en ansvarlig i virksomheden
- Fastlæg indsatsområder og prioritér
- Anerkend at persondata er noget, der er kommet for at blive = vedligeholdelse fremover er vigtigt
- Awareness hos medarbejdere

ADVODAN

ADVODAN – WORKSHOPS (''HJÆLP TIL SELVHJÆLP'')

- Det er svært tilgængeligt stof for de fleste og det kan være svært at vælge og prioritere indsatsområder

- Forløb med 4-6 workshops med fokus på et par temaer ad gangen har vist sig effektivt. Rådgivning / sparring i mindre grupper, hvorefter man går hjem i sin virksomhed og arbejder videre. Næste møde nyt tema indtil man er i gennem…

ADVODAN