Personvernombudsordningen etter GDPR

Ove Skåra - Datatilsynet

Datatilsynet

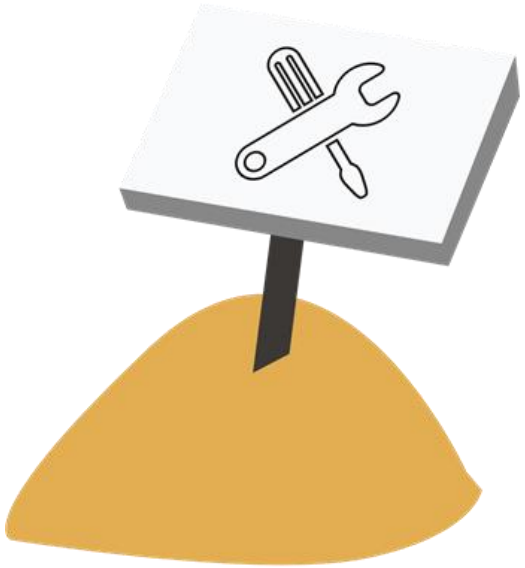
Viktigste endringer

- Fremhevet og lovregulert
- Skjerpede krav og tydeligere rolle
- Fra frivillig til obligatorisk for mange

- Artikkel 37, 38 og 39 i forordningen
- Retningslinjer fra WP29

Oppgaver

- Samle inn og ha oversikt over behandlingsaktiviteter
- Involvere seg tidlig, informere og gi råd
- Kontrollere overholdelse av personvernregelverket og interne retningslinjer, deriblant ansvarsfordeling, opplæring, holdningsskapende tiltak mv,
- Gi råd og delta ved vurdering av personvernkonsekvenser (DPIA)
- Være kontaktpunkt for de registrerte
- Være et kontaktpunkt for, og samarbeide med Datatilsynet
- Skal ha en risikobasert tilnærming til sitt arbeide



Mao: En viktig støttende funksjon for å sikre behandlingsansvarliges etterlevelse av kravene i personvernlovgivningen, men PVO overtar ikke behandlingsansvarliges rolle eller ansvar!

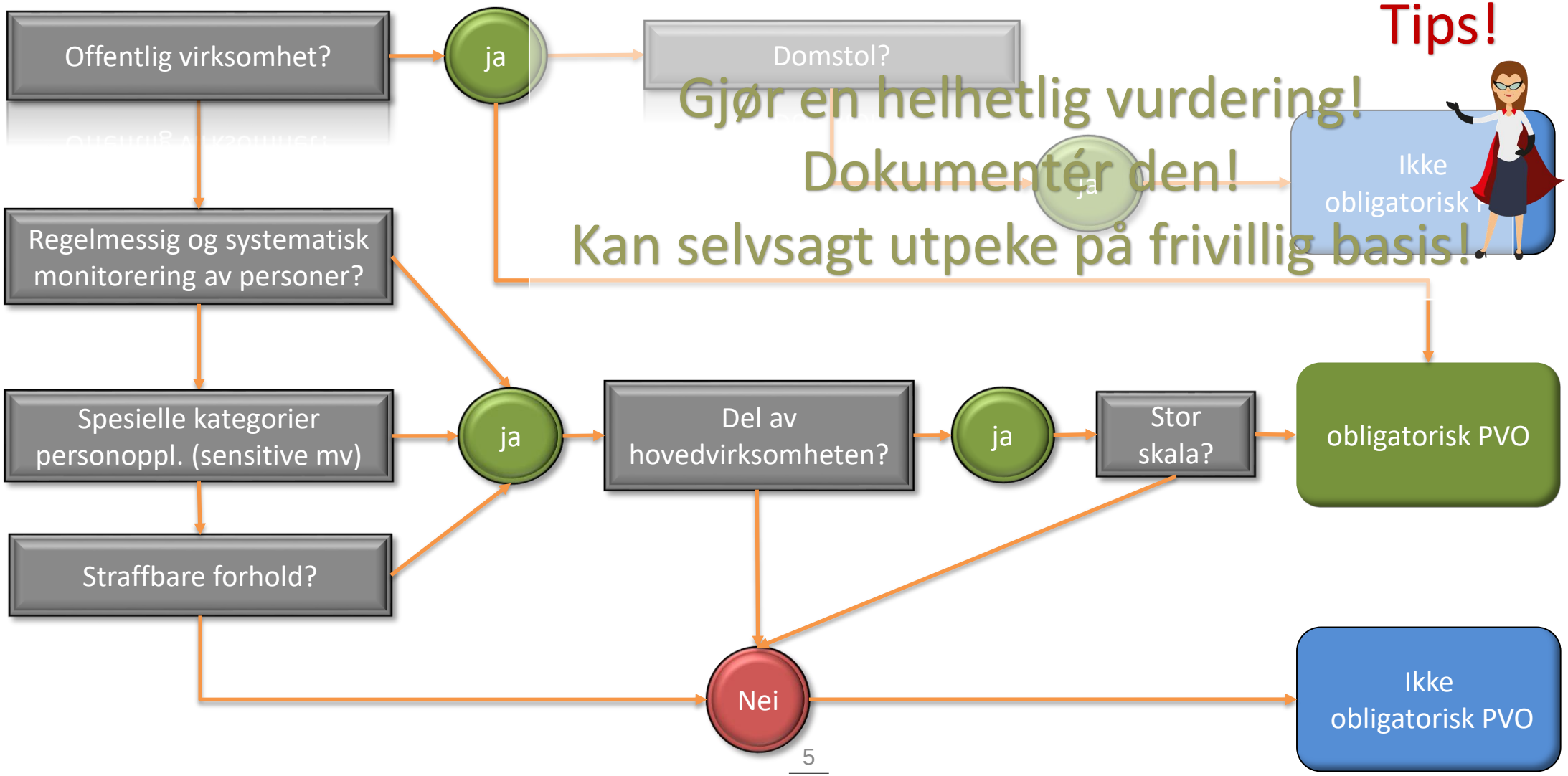
Art. 39

Hvem er personvernombud obligatorisk for?

1. offentlige myndigheter og organer (unntatt domstolene)
2. behandlingsansvarlige og databehandlere der hovedvirksomheten består av behandlingsaktiviteter som på grunn av sin art, sitt omfang eller formål krever regelmessig og systematisk monitorering i stor skala av registrerte, eller
3. hovedvirksomheten består av behandling av sensitive personopplysninger i stor skala, eller personopplysninger knyttet til straffbare forhold.

Art. 37

Obligatorisk med personvernombud i vår virksomhet?



Hva menes med monitorering

- «For å fastslå om en behandlingsaktivitet kan anses som monitorering av de registrertes atferd bør det bringes på det rene om det skjer sporing av fysiske personer på internett, herunder en mulig påfølgende bruk av teknikker for behandling av personopplysninger som innebærer profilering av en fysisk person, særlig med det formål å treffe beslutninger om vedkommende eller analysere eller forutsi vedkommendes personlige preferanser, atferd eller holdninger.»

Fortalen, punkt 24

Hva menes med monitorering?

- Monitorering omfatter alle former for sporing og profilering av personer på nettet, inklusive persontilpasset reklame.

- Begrepet begrenses imidlertid ikke bare til aktiviteter på internett

- Eksempler:
  - Drift av et telekommunikasjonsnettverk
  - Målrettet e-postreklame
  - Profilering og vurdering i forbindelse med kredittvurdering
  - Sporing av lokasjon i mobilapplikasjoner
  - Monitorering ved bruk av helsearmbånd
  - Bruk av internettilknyttede enheter, som for eksempel smarte biler, automatiske strømmålere, smarthus og lignende
  - Kundeklubber eller lojalitetsprogrammer
  - Kameraovervåking

WP29

«Regelmessig og systematisk» monitorering

Regelmessig:

- Pågående eller skjer jevnlig i en bestemt periode
- Gjentakelse på faste tidspunkt

Systematisk:

- Skjer etter et system
- Forhåndsbestemt, organisert eller metodisk
- Som en del av en generell plan for datainnhenting
- Som en del av en strategi

WP29

Sensitive opplysninger og straffbare forhold

- Sensitive opplysninger/særlige kategorier av personopplysninger (art. 9):
  - rasemessig eller etnisk opprinnelse
  - politisk oppfatning
  - religiøs eller filosofisk overbevisning
  - Fagforeningsmedlemskap
  - behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person
  - Helseopplysninger
  - opplysninger om en fysisk persons seksuelle forhold eller seksuelle legning
- Straffbare forhold (art. 10):
  - personopplysninger i forbindelse med straffedommer og straffbare forhold eller tilknyttede sikkerhetstiltak

Hva er «hovedvirksomhet»?

- «Hovedvirksomhet» er kjerneaktiviteter som er nødvendig for å oppnå virksomhetens mål.

- Skillelinje: Hvis behandling av personopplysninger er uløselig forbundet med virksomhetens produkt/tjeneste? Hvis ja: hovedvirksomhet.

WP29

Personopplysninger som del av hovedvirksomhet?

- Et sykehus sin hovedvirksomhet er å gjøre folk friske, men kan ikke gjøre det uten å behandle personopplysninger.

- Et sikkerhetsselskap utfører videoovervåking på flere kjøpesentre. Å sørge for sikkerheten er hovedvirksomheten, men kan ikke skilles fra behandlingen av personopplysninger.

Begge disse er derfor pålagt å opprette personvernombud

WP29

Biaktiviteter

- Noen aktiviteter er standard i alle organisasjoner. Selv om disse er viktige, blir de i denne sammenheng sett på som biaktiviteter:
  - Personaladministrasjon
  - Standard IT-støtte

WP29

Hva menes med «stor skala»?

- Følgende faktorer bør vurderes for om en behandling er i stor skala:
  - Antallet personer det behandles data om (faktisk antall eller andel av en populasjon)
  - Mengden data og/eller omfanget av dataene som blir behandlet
  - Varigheten av behandlingen, og om den er permanent
  - Det geografiske omfanget av behandlingen

WP29

Eksempler på stor skala

Stor skala:

- Sykehus
- Offentlige transportsystemer i en by
- Banker
- Forsikringsselskaper
- Søkemotorer (for å gi tilpasset reklame)
- Teletilbydere

Ikke stor skala:

- Enkeltstående fastlege
- Advokat som jobber i enkeltmannsforetak

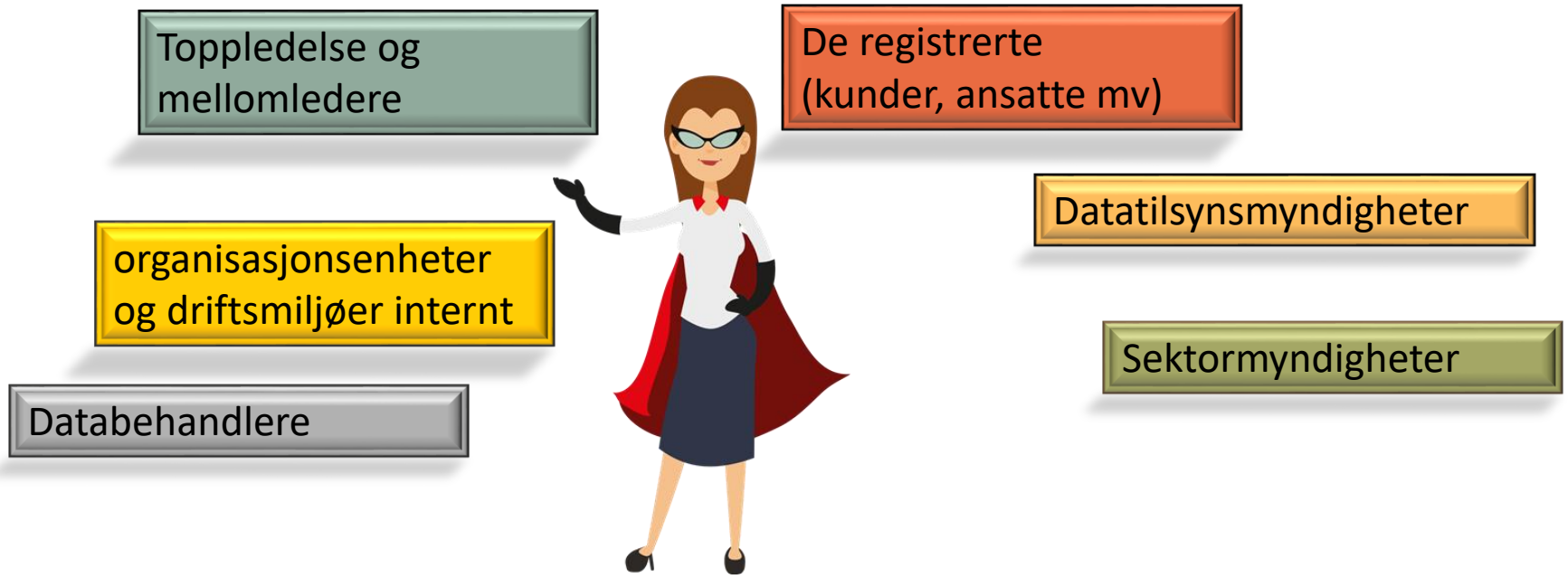
WP29

Om utpeking av personvernombud

- Både behandlingsansvarlige og databehandlere er omfattet av reglene
- Konserner kan ha felles ombud for underliggende virksomheter og offentlige etater kan oppnevne felles ombud
  - Må være forsvarlig mht tilgang til vedkommende, og mht struktur, størrelse på virksomhetene og omfang og kompleksitet
- Kan kjøpe PVO som ekstern tjeneste
- Ikke mer enn ett ombud i en og samme virksomhet

Art. 37

Må finne balanse mellom flere ulike interessenter



Hva slags kvalifikasjoner må ombudet ha?

- **Faglige og formelle kvalifikasjoner**
  - bør stå i forhold til skala og kompleksitet
- **Dybdekunnskap om personvernlovgivning og praksis på området**
  - Kjennskap til sektoren og forståelse av behandlings-aktivitetene, IT-systemer, informasjonssikkerhet mv.
- **Evne til å utføre oppgavene**
  - Personlige kvaliteter og kunnskap
  - Posisjon i virksomheten
  - Personlig integritet og evne til å gjøre etiske vurderinger
  - Evne til å kommunisere og stimulere resten av organisasjonen

Art. 37

Virksomhetens ansvar mht personvernombudet

- Skal sørge for at personvernombud blir utnevnt iht kravene
- Må involveres i prosesser
- Skal få ressurser og tilgang til informasjon og systemer
- Skal ha mulighet til å opprettholde sakkunnskap
- Respektere den uavhengige rollen. Skal ikke motta instrukser eller straffes
- Skal rapportere til høyeste ledelsesnivå
- Må ikke ha andre oppgaver som fører til interessekonflikt
  - Kan ikke ha stilling som innebærer at ombudet skal bestemme formålet og metode for behandling av personopplysninger

Art. 38

Datatilsynets rolle og planer

- Skal ikke lenger behandle søknader om ombud
- Skal få beskjed om hvem som er ombud
  - Mål om å ha offentlig oversikt
- Tilpasset opplæring i 2017 og 2018(?)
- Er i kontakt med eksterne utdanningsaktører om fremtidig kursing
- Informasjon til ombud og virksomheter som må ha ombud