Nye personvernregler fra 20. juli 2018

Fagdag Fagforbundet

Knut B. Kaspersen - Datatilsynet

6. september2018

Datatilsynet

Personopplysninger – hva er det?

Peder Aas
2020 Lillevik

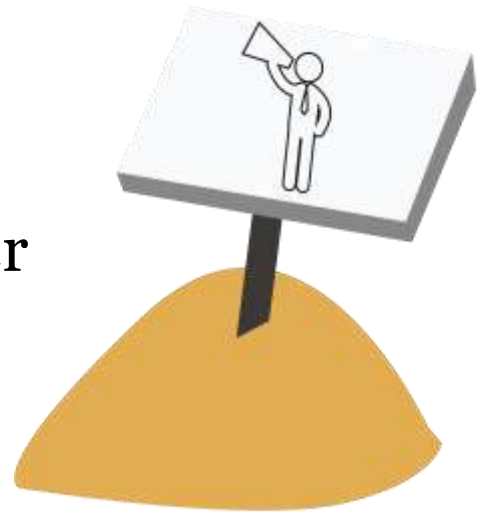
F.nr 180262 34997

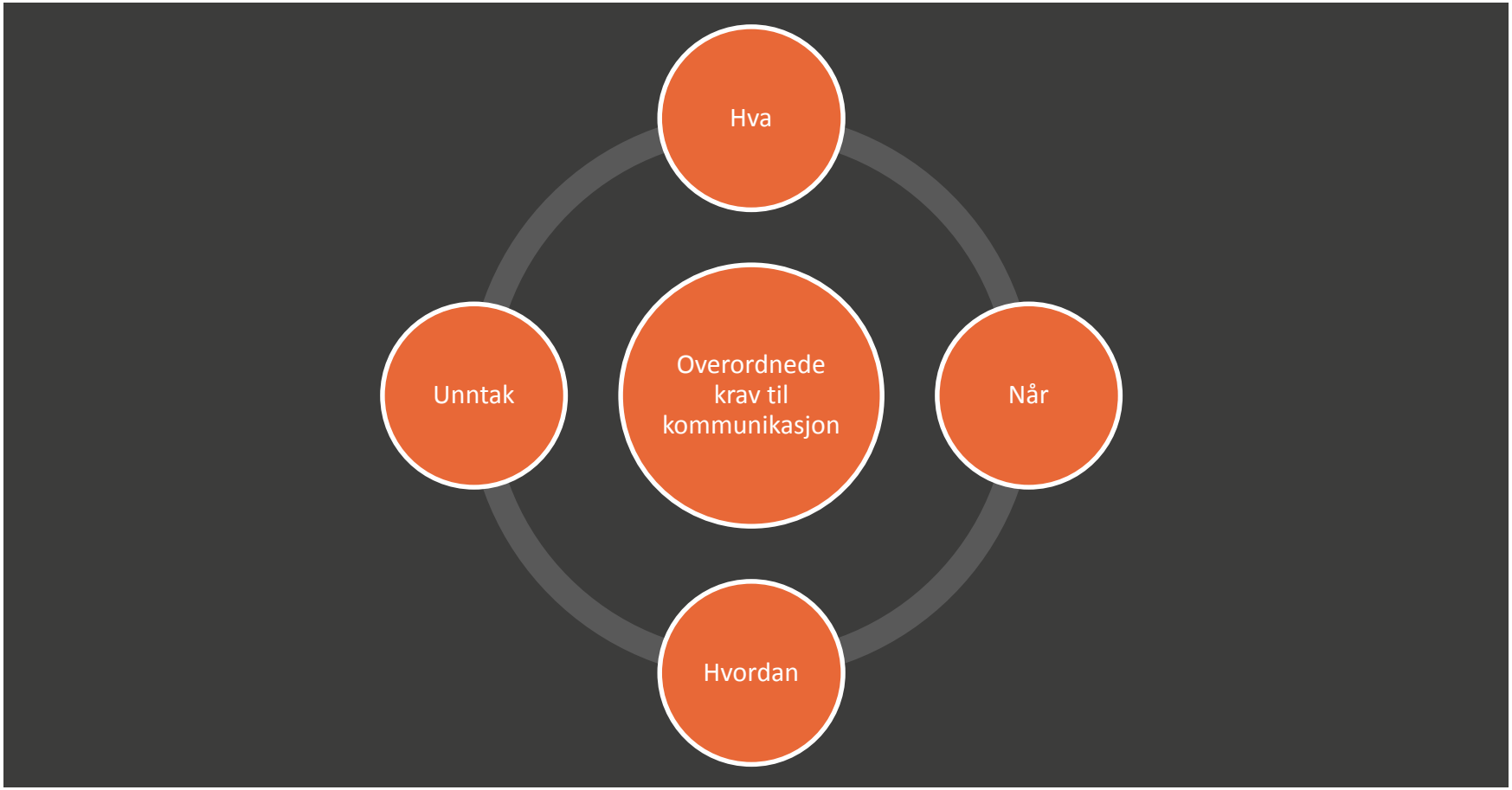
Hva er personopplysninger?

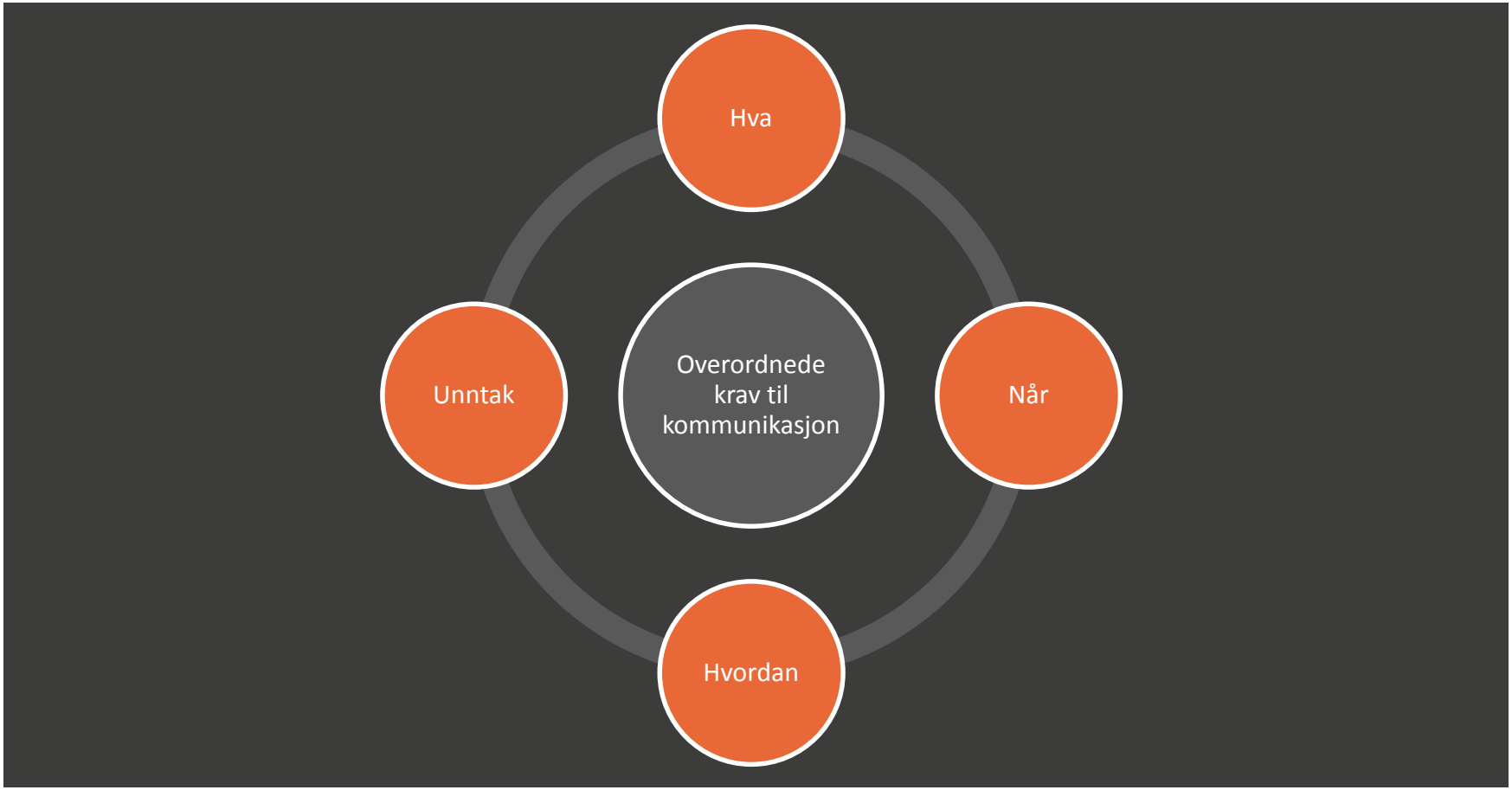
Personopplysninger – hvor er de?

Informasjon til de registrerte skal gis i klarspråk

- Informasjonen skal være lett tilgjengelig
- Klart språk som er tilpasset leserens nivå
- Stilles krav til hvilke opplysninger som skal gis
- Informasjonen kan erstattes med ikoner art 12 nr. 7
- Personvernerklæring godt alternativ




Hva
Unntak
Overordnede krav til kommunikasjon
Når
Hvordan


Hva
Unntak
Overordnede krav til kommunikasjon
Når
Hvordan

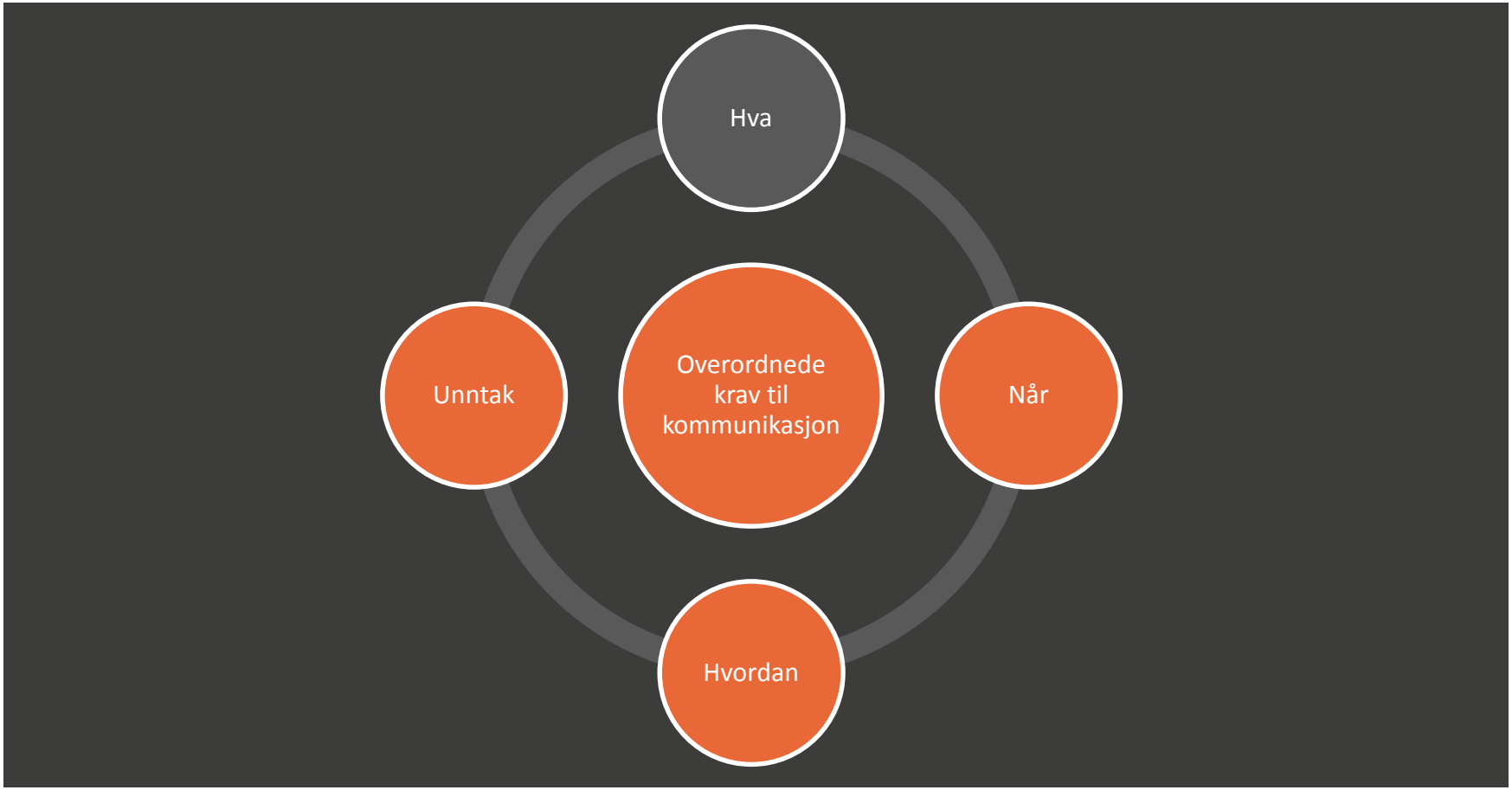
Overordnede krav til kommunikasjon

- Hva er kommunikasjon?
  - Informasjon (type personvernerklæringer)
  - Utøvelse av rettigheter
  - Underretning om avvik

- Hvilke krav stilles?
  - Kortfattet
  - Åpen
  - Forståelig
  - Lett tilgjengelig
  - Klart og enkelt språk, især når rettet mot barn

Overordnede krav til kommunikasjon

- Hva betyr det i praksis?
  - Ikke juridisk eller teknisk sjargong
  - Forståelig for målgruppen og ha god struktur
  - Informasjonen skal være konkret (ikke «vi *kan* bruke personopplysninger til …»)
  - Adskilt fra annen informasjon (for eksempel brukervilkår).
  - Skal ikke måtte lete etter informasjon
  - Lett å finne frem i informasjonen
  - Må ikke sette seg inn i store mengder informasjon


Hva
Unntak
Overordnede krav til kommunikasjon
Når
Hvordan

Hva

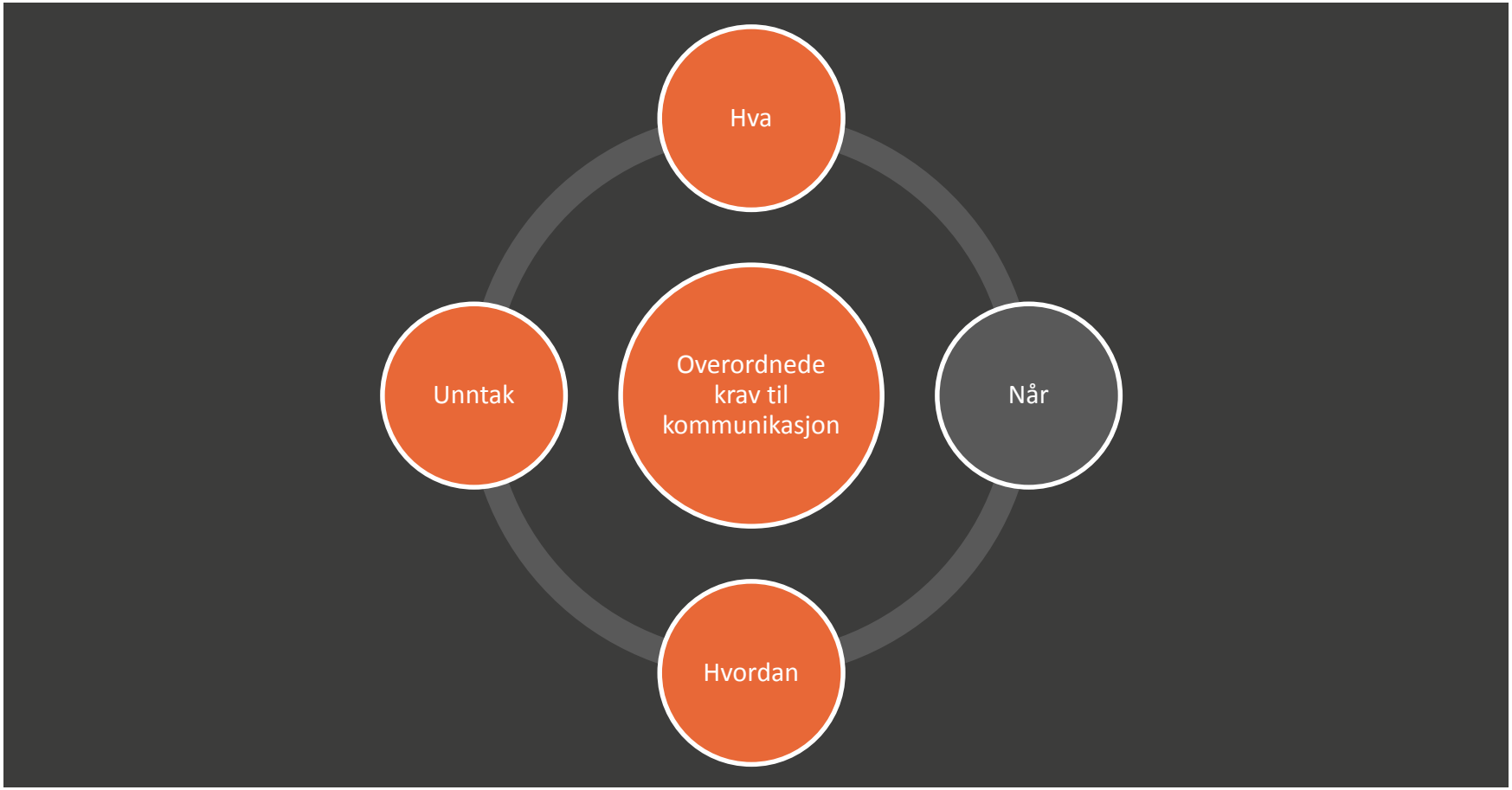
- Om virksomheten
- Om behandlingen
- Om forholdet til andre virksomheter

Hva

- Om den enkeltes rettigheter
- Om automatiserte individuelle avgjørelser
- Om nye formål

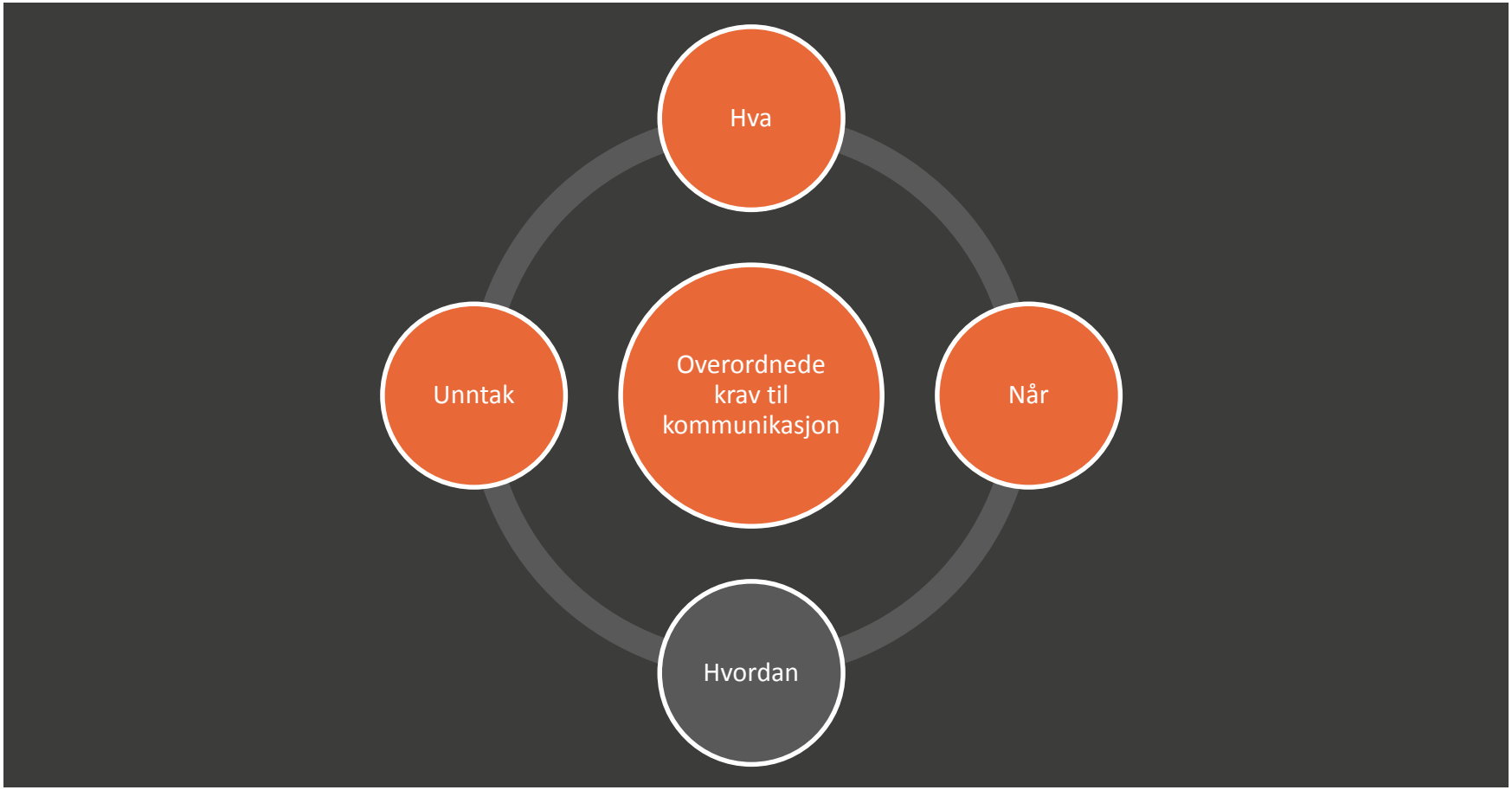
Hva

- Om konsekvenser
- Om endringer


Hva
Unntak
Overordnede krav til kommunikasjon
Når
Hvordan

Når

- Innhentet fra den registrerte/observert
  - Når personopplysninger samles inn
- Innhentet fra andre kilder enn den registrerte
  - Rimelig tid, men senest én måned
  - Ved første kommunikasjon, men senest én måned
  - Når utlevering skjer, men senest én måned
- Berørt ved avvik art. 34


Hva
Unntak
Overordnede krav til kommunikasjon
Når
Hvordan

Hvordan

- Prinsippene avgjør

Hvordan

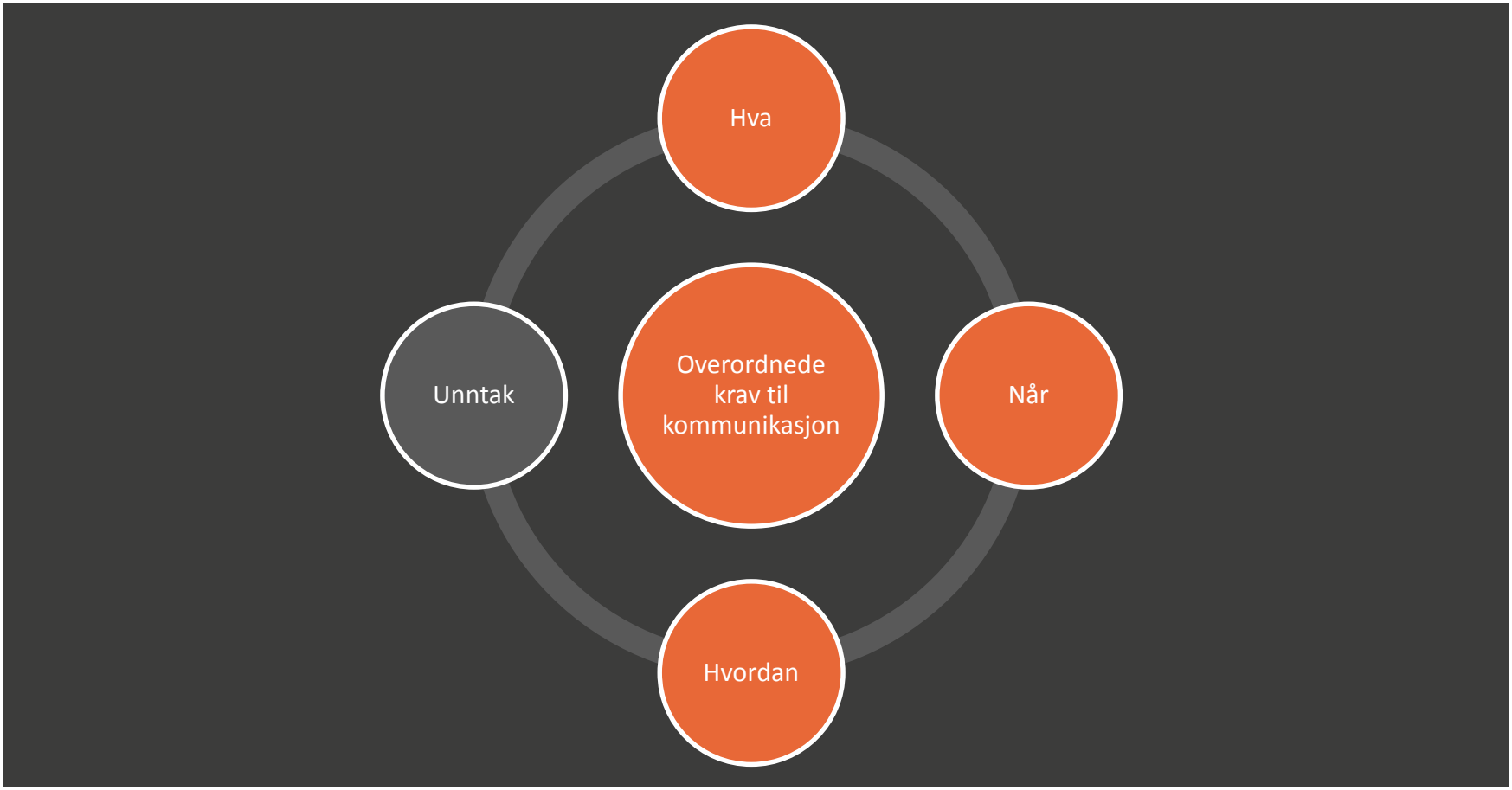
- Formkrav
  - Skriftlig
  - Mixed media
  - Muntlig

- Oppbygging
  - Lagvis informasjon
  - Strukturert og oversiktlig
  - Første lag
    - Formål
    - Virksomhetens identitet
    - Den registrertes rettigheter
    - Behandling av personopplysninger som kan ha særskilt stor innvirkning på den enkelte, overraskende
    - Rettferdighetsprinsippet

Hvordan

- Modalitet
  - Dytt-informasjon
  - Dra-informasjon

- Akkurat-i-tide-informasjon
- Personvernkontrollpanel
- «Mouseover»
- «3D Touch»
- Samlet informasjon
- Elektronisk tjeneste, elektronisk informasjon


Hva
Unntak
Overordnede krav til kommunikasjon
Når
Hvordan

Unntak

- Tre unntakstyper
  - Når innhentet fra den registrerte/observert
  - Når innhentet fra andre kilder enn den registrerte
  - Generelle, særnorske unntak

Unntak

- Innhentet fra den registrerte/observert
  - Ikke nødvendig hvis og i den grad den enkelte allerede har informasjonen
  - Ansvarlighetsprinsippet gjelder – dersom virksomheten påberoper seg unntaket, må den kunne godtgjøre at den enkelte har informasjonen og at den er oppdatert
  - Supplere/gi alt på nytt

Unntak

- Innhentet fra andre kilder: Dersom og i den grad
  - den enkelte allerede har informasjonen
  - det er umulig å gi informasjonen*
  - det vil innebære en uforholdsmessig stor innsats å gi informasjonen*
  - informasjon sannsynligvis vil umuliggjøre eller i alvorlig grad hindre formålet med behandlingen*
  - innsamling eller utlevering har en uttrykkelig hjemmel i lov som virksomheten er underlagt og som inneholder egnede tiltak for å verne den enkeltes interesser
  - personopplysningene må holdes konfidensielle som følge av taushetsplikt

Unntak

- Generelle, særnorske unntak
  - utenrikspolitiske interesser, forsvars- og sikkerhetsinteresser
  - forebygging, etterforskning, avsløring og rettslig forfølgning av straffbare handlinger
  - det må anses utilrådelig at den enkelte får kjennskap til opplysningene av hensyn til vedkommendes helse eller forholdet til personer som står vedkommende nær
  - taushetsplikt
  - intern saksforberedelse
  - det vil være i strid med åpenbare og grunnleggende private eller offentlige interesser å informere

Innsynsretten

- GDPR art. 15

- Alle har rett til:
  - å vite om virksomheten behandler dine personopplysninger
  - informasjon om behandlingen
  - gratis kopi av alle opplysningene

- To testpersoner har testet innsynsretten. Hva vet virksomhetene om deg?

Hva vet de om deg?

Hva du ser på TV

Hvor du har vært

Hvilke nyhetsartikler du leser og hva du kjøper og selger på finn.no

Hva slags utdannelse du har

Inntekt og formue

Hvem du ringer og tekster og når du bruker mobilen

Hva du legger i handlevogna – dette kan igjen si noe om helsen din

Hva vet de om deg?

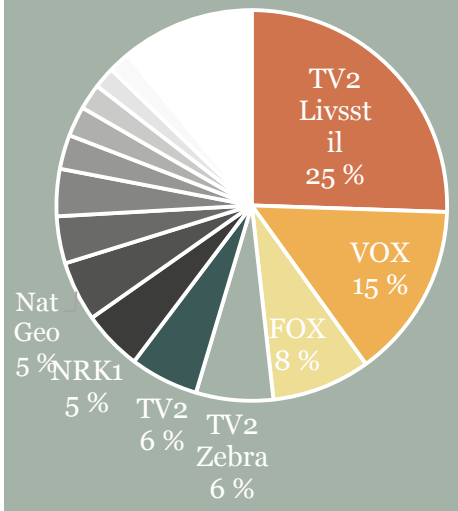
- Testperson ba om innsyn hos et TV-selskap
- Fikk tilbake en oversikt over hvilke kanaler og programmer han hadde sett på
- TV-selskapet hadde i tillegg profilert testpersonen
  - Antatt inntekt og formue
  - Antatt boligtype
  - Antatt utdannelse
  - Antatt samlivsform og antall barn

Testpersonens mest sette TV-programmer

1. Keeping Up with the Kardashians
2. The Good Wife
3. Alaska siste utpost
4. Ødemarkens menn
5. Mord og mysterier

Testpersonen har også sett mye på serier om interiør og veterinærer.

Testpersonens mest sette TV-kanaler



Hva vet de om deg?

- Testperson ba Schibsted (Aftenposten, VG, Finn) om innsyn
- Fant ut at alt man gjør på nettavisene og Finn analyseres
- 7 millioner datapunkter fra 400 000 interaksjoner
- Hva man leser og søker etter forteller mye

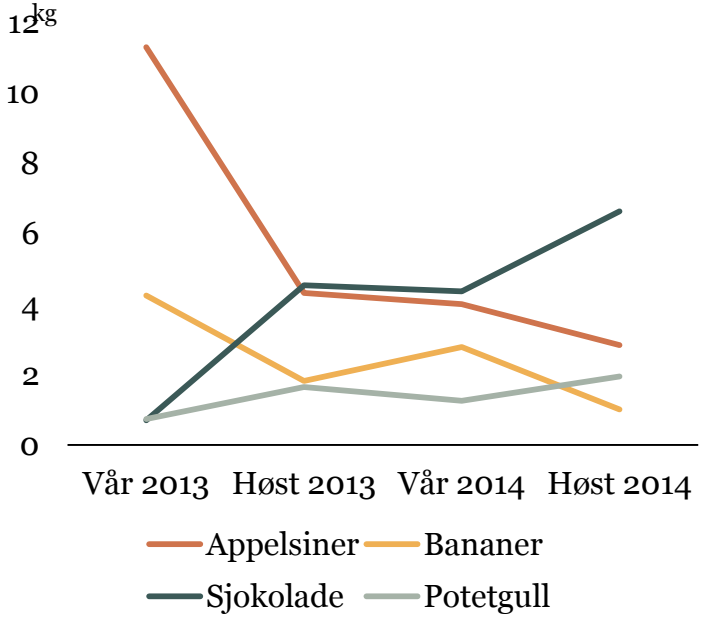
Hvem er testpersonen?

- Interessert i boligannonser i Oppegård og Ski.
- Personen har søkt etter barnevogn på finn.no. Er det familieforøkelse på gang?
- Testpersonen leste en stillingsannonse på finn.no på en Samsung-mobil den 8. september 2015 klokken halv ti om morgenen. Skal han slutte i Datatilsynet?
- Vi kan se hvor ofte testpersonen bommer på tastene når han skriver inn søkeord på finn.no.
- Testpersonen brukte bare 53 sekunder på å lese en artikkel om hvorfor man bør dusje rett etter trening. Til sammenlikning brukte han 10 minutter og 43 sekunder på en artikkel om Magnus Carlsen.
- Vi vet personen var våken og leste nyheter klokka 06.06 den 8. november 2016. Han var fremdeles våken klokka 22.23.
- Søndag 26. juli 2015 var vedkommende i Strømstad. (Lurer på hva han gjorde der?)

Hva vet de om deg?

Hva vet de om deg?

- Testperson ba om innsyn hos dagligvare-kundeklubb
- Full handlehistorikk fem år tilbake i tid
- Hva du legger i handlekurven sier mye
  - Kosthold (helse, religion)
  - Alkohol, tobakk og kondomer
- Ble plassert i ulike segmenter



Hva vet de om deg?

- Testperson ba om innsyn hos teleoperatør
- Teleoperatører lagrer *metadata*
- Unike data – metadata-fingeravtrykk
- Teledata kan havne på avveier

Sikkerhet ved behandling – art. 32

- Risikovurdering
- Sikkerhetstiltak
  - Pseudonymisering og kryptering av personopplysninger
  - Sikre vedvarende K, I, T og robusthet
  - Gjenoppretting av tilgjengelighet og tilganger ved hendelser
  - Jevnlig testing, vurdering og evaluering
- Bransjenormer eller godkjent sertifiseringsordning
  - Element for å vise etterlevelse
- Tiltak for å sørge for at behandling kun skjer på instruks fra behandlingsansvarlig

Sikkerhet ved behandling – art. 32

- Artikkelen er mer utfyllende enn dagens § 13, men mindre konkret enn kap. 2 i forskriften. Vi finner allikevel igjen mange av pliktene i teksten og har sett på sammenfallende krav fra alle pliktene i forskriften til artikkel 32.
- Nytt er robusthet og «state of the art».
- Dokumentasjon er ikke spesifikt nevnt, men her vi finner en universell plikt i artikkel 24 (internkontroll).

Avvik art. 33

Eksempler:

Politiske parti

Bruk av minnepenn

Tyveri av bærbar PC

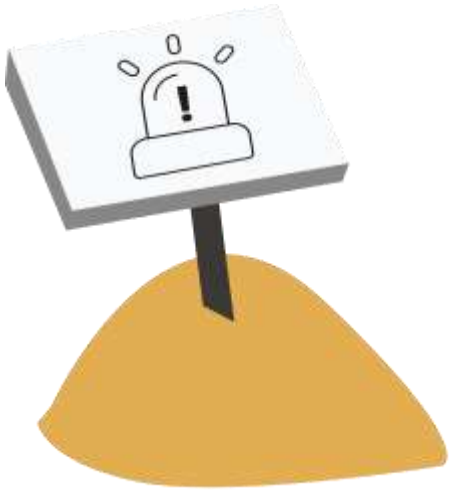
St. Olavs Hospital

Ålesund kommune

Andebu kommune

Råde kommune

Avviksmeldinger – art. 33

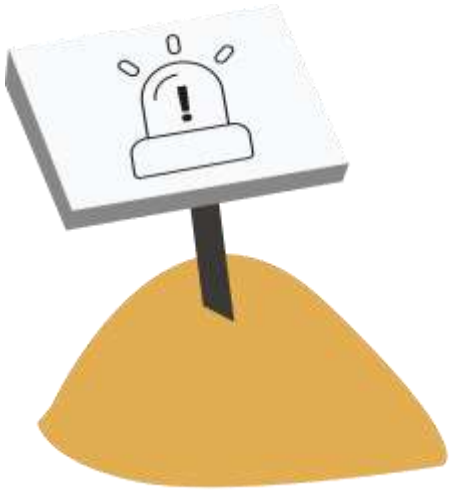


Sikkerhetsbrudd (art. 4 (12)):
«brudd på personopplysningssikkerheten» - er et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet

Dette omhandler mer enn dagens § 2-6 tredje ledd:

«uautorisert utlevering av personopplysninger som krever konfidensialitet»

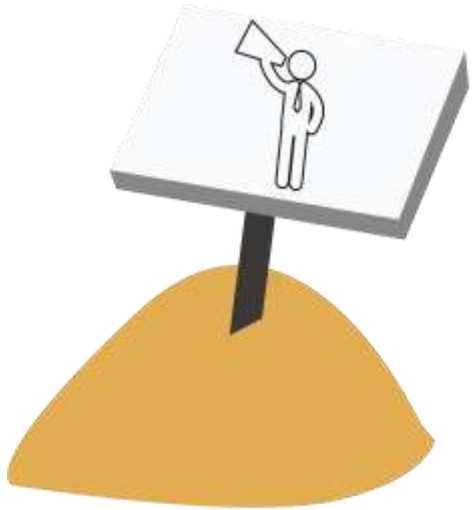
Avviksmeldinger – art. 33



- Behandlingsansvarlig må melde avvik innen 72 timer. Kan meldes trinnvis.
- Databehandler melder til behandlingsansvarlig
  Uklart: kan en databehandler melde inn på vegne av flere behandlingsansvarlige?
- Stilles krav til innholdet i avviksmeldingen. Vårt skjema i Altinn tar høyde for dette. Lanseres når Altinn har et «vindu»…
- Finnes en uttalelse fra Artikkel 29-gruppen (2014) som skal oppdateres i løpet av året. Gjelder både artikkel 33 og 34.

Informasjon til de berørte – art. 34

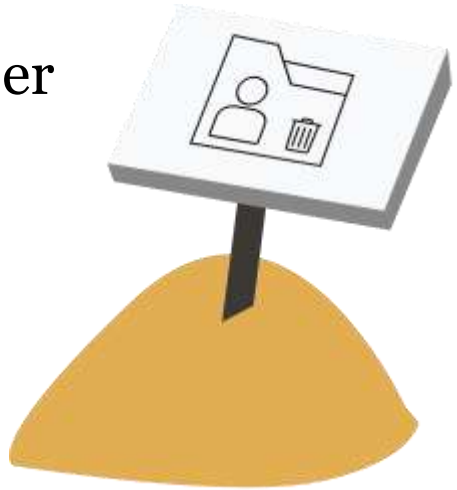
- Kravet finnes ikke i dagens regelverk, men ny praksis er gått opp med «GE-sakene» i Personvernnemnda (artikkel på datatilsynet.no)
- Berørte skal informeres så raskt som mulig, slik at de skal kunne foreta seg noe for å begrense skaden.



- Unntak i kravet om varsling:
  - Eksisterende tiltak som gjør informasjonen uleselig, f.eks. kryptering
  - Tiltak i ettertid som sikrer at den høye risikoen ikke lengre vil oppstå (er til stede)
  - Uforholdsmessig innsats. Må i stedet informere offentlig eller tilsvarende.

Alle må kunne oppfylle borgernes nye rettigheter

- Retten til å bli glemt
- Rett til at personopplysninger begrenses
- Systemer må oppfylle krav til dataportabiliet
- Strengere regler for automatiserte avgjørelser
- Håndtere henvendelser fra borgere innen 1 måned



Hva bør alle virksomheter gjøre nå?

- Sørge for å ha oversikt over hvilke personopplysninger de behandler
- Sørge for å oppfylle dagens lovkrav
- Sette seg inn i det nye regelverket
- Lage rutiner for å følge de nye reglene

Datatilsynet.no/forordning

Nye personvernregler fra 2018

Hva betyr det for din virksomhet?

Datatilsynet

Til ledere med ansvar for personvern, sikkerhet og utvikling

Er du klar for nytt regelverk?

I 2018 blir dagens personvernregelverk erstattet av EUs personvernforordning. Norske virksomheter bør derfor begynne å forberede seg på nye personvernregler allerede nå. Før de nye reglene trer i kraft må dere sørge for at dere har:

1 Internkontroll og oversikt over hvordan dere behandler personopplysninger

Fra 2018 må ikke bare behandlingsansvarlige, men også databehandlere ha oversikt over behandling av personopplysninger.

2 Systemer, tjenester og løsninger som oppfyller prinsippene om innebygd personvern

Velg den mest personvennvennlige innstillingen som standard. Bygg personvernet inn ved blant annet å begrense mengden informasjon som samles inn, pseudonymisere opplysninger så raskt som mulig, være åpen om innsamling og bruk av opplysninger, og tenke sikkerhet i alle utviklingsfaser (innebygd sikkerhet).

3 Systemer som er tilpasset for dataportabilitet

Alle registrerte skal som hovedregel kunne ta med seg personopplysninger de selv har oppgitt, fra en virksomhet til en annen. Systemene dere bruker må være tilpasset for overføringer og mottak av opplysninger.

4 Tilstrekkelig informasjonssikkerhet

Gjennomfør risikovurderinger og få på plass tekniske og organisatoriske tiltak som pseudonymisering og kryptering. Systemene må sikre konfidensialitet, integritet, tilgjengelighet og robusthet. Sørg for at tilgjengelighet og tilgang til personopplysningene dere behandler gjenopprettes på en sikker måte etter hendelser. I tillegg må dere ha prosedyrer for å teste, vurdere og evaluere at tiltakene både er effektive og ivaretar sikring av alle personopplysninger virksomheten behandler.

5 Rammeverk og rutiner for å vurdere personvernkonsekvenser

Dersom et tiltak er inngripende, skal dere vurdere personvernkonsekvensene ved tiltaket ved hjelp av en Privacy Impact Assessment (PIA) før det iverksettes. Er risikoen høy og umulig for dere å redusere, skal Datatilsynet involveres i forhåndsdrøftelser.

6 Rutiner for avviksbehandling

Forordningen stiller strengere krav til avviksbehandling enn dagens regelverk. Ved brudd på sikkerheten skal dere varsle Datatilsynet innen 72 timer, og vi skal varsles oftere enn før. I tillegg skal dere informere alle som er berørt av sikkerhetsbruddet. Databehandlere skal også varsle behandlingsansvarlig umiddelbart ved avvik.

datatilsynet.no/forordning

Datatilsynet