Nye personvernregler fra mai 2018

Arkivlederseminar 2017 IKA Kongsberg

Knut B. Kaspersen - Datatilsynet

25. oktober 2017

Datatilsynet

Personvern

- Hva er det

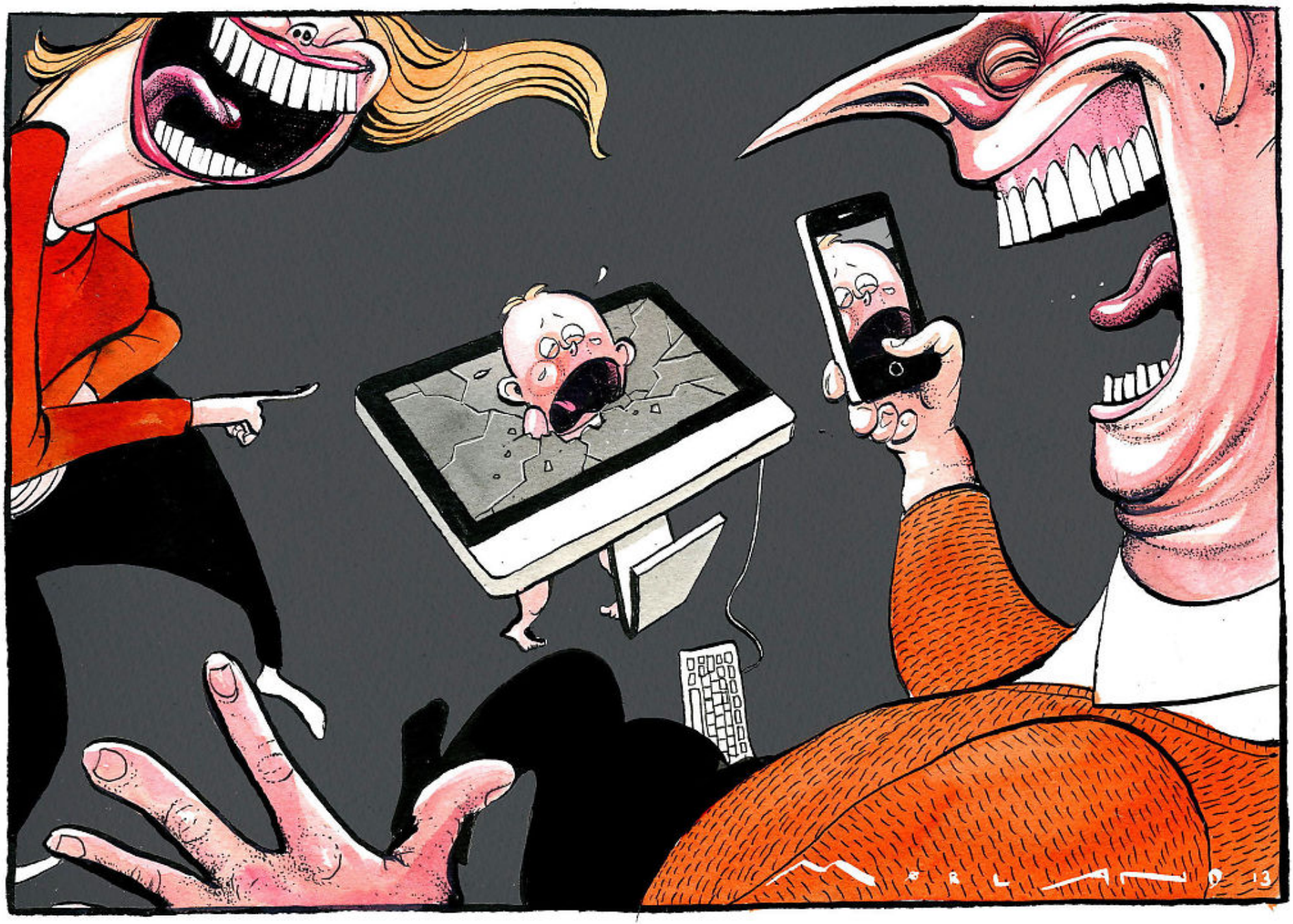

MORLANO 13

Foto: REUTERS

PARTERINGSDRAPET

La ut likbilder på Snapchat

OFFER: *Politiet mener Sami Milhem ble utsatt for et hevndrap. Han ble drept med kniv.*
Foto: NTB SCANPIX

Av GORDON ANDERSEN, BJØRNAR TOMMELSTAD og OLA MJAALAND

Politiet måtte slette bilder som vitner tok av den drepte Sami Milhem (20) da han ble funnet partert og drept tidligere i sommer.

20-åringen Sami Milhem ble funnet ille tilredt i en leilighet i Hareid fredag 8. august. Politifolkene som kom til stedet kunne raskt se at han manglet flere kroppsdeler.

Da politiet tok seg inn i leiligheten hvor han ble funnet, oppdaget de at flere vitner hadde tatt bilder av liket og sendt på sosiale medier, blant annet på delingstjenesten Snapchat.

Snapchat er en billeddelingstjeneste hvor bildet bare er synlig i noen få sekunder for mottageren, med mindre mottageren kopierer bildet. Bildene ble også, etter det VG får opplyst, sendt på vanlig MMS.

Oppdagelsen gjorde at politiet måtte gå hardt til verks og slette bildene fra mobiltelefonene til dem som hadde fotografert.

Frykten var at bildene i verste fall skulle bli kjent for familien til den drepte, eller at media skulle få tak i dem, får VG opplyst.

– Uten nettvett

VG har vært i kontakt med bistandsadvokat Jørund Knardal. Han representerte familien til den drepte da saken var i innledningsfasen, før familien flyttet til Sørlandet.

– Dette synes jeg er helt forkastelig. Personer som gjør noe slik mangler alt som er av nettvett. Det hadde vært grusomt for familien om de skulle ha blitt kjent med dette bildet av sin sønn, sier Knardal til VG.

Advokat: Dette er forkastelig

Oppdagelsen gjorde også at politiet tidlig gikk ut i media og opplyste at 20-åringen var blitt partert.

– I begynnelsen var politiet veldig tilbakeholdne, men lørdag morgen 9. august ble familien varslet om det som skulle komme frem i pressemeldingen rett etterpå, sier Knardal.

Det var da politiet gikk ut med detaljer om at avdøde manglet flere kroppsdeler. Senere fikk familien flere detaljer fra obduksjonsrapporten.

Kniv i container

Politiet nærmer seg avslutningen i etterforskningen av det bestialske Hareid-drapet. En rekke politifolk fra Kripos har bistått lokalt politi i det krevende etterforskningsarbeidet.

Ifølge politiets etterforskning skal det være avklart at de står overfor et hevndrap.

Politiet har også funnet drapsvåpenet. Det er en ganske stor kniv, som politiet fant dumpet i en container i nærheten av Eurosparbutikken på Valderøya.

– Den siktede mannen var innom butikken vår og handlet. Vi hjalp politiet med å finne overvåkningsbilder. Politiet fant senere en søppelsekk i en container ved butikken, som de viste stor interesse for, sier Hans Idar Valderhaug, nestleder i Eurospar Valderøy.

Politiet fant drapsvåpenet etter å ha sett overvåkningsbilder fra butikken, der de kunne se gjerningsmannen kaste fra seg kniven i en søppelbøtte utenfor. Søppelet ble senere tømt i containeren uten at noen oppdaget kniven.

Den 23 år gamle mannen fra Nordland som er siktet for å ha drept og partert Sami Milhem (20), har erkjent de faktiske forholdene rundt drapet og samtykket til varetektsfengsling.

E-post: gordon.andersen@vg.no

What is personal data?

COLLECT
STORE
USE
DATA?

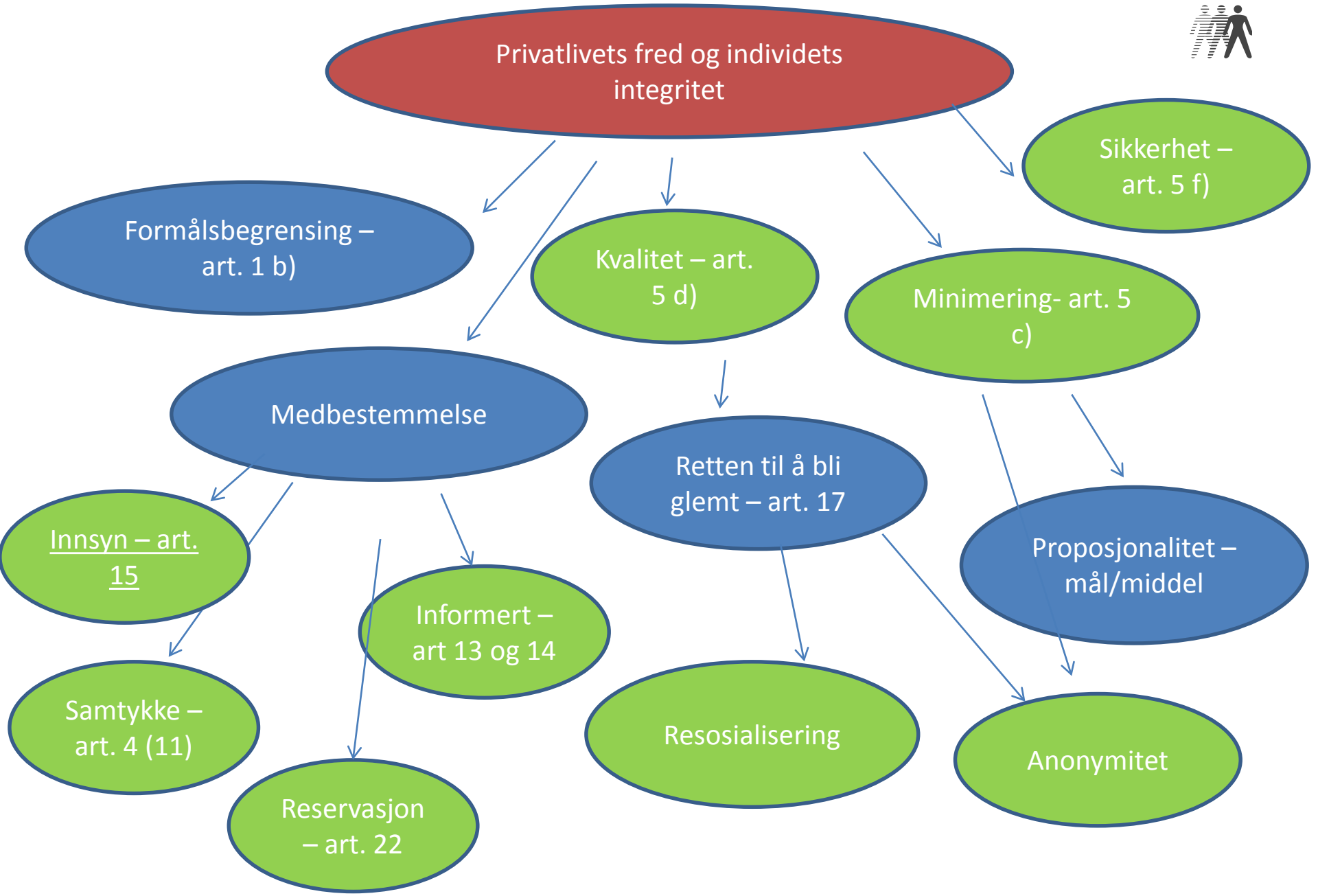
You have to abide by the rules.


ON YOUR MARK
GET READY
ANY TIME NOW
REALLY SOON...
GDPR


General
Data
Protection
Regulation

Viktig nytt i forordningen

- Materielle krav i regelverket:
  - ✓ Innebygd personvern og personvern som standard innstilling
  - ✓ Vurdering av personvernkonsekvensene
  - ✓ Mer tydelige krav til informasjon og samtykke
  - ✓ Mye strengere sanksjoner
- Strategier for etterlevelse av regelverket:
  - ✓ Obligatorisk personvernombud
  - ✓ Risikobasert *accountability*
  - ✓ Forhåndsdrøftelser
  - ✓ Bransjenormer og sertifisering
  - ✓ Europeisk samarbeid


Privatlivets fred og individets integritet
Sikkerhet – art. 5 f)
Formålsbegrensing – art. 1 b)
Kvalitet – art. 5 d)
Minimering- art. 5 c)
Medbestemmelse
Retten til å bli glemt – art. 17
Innsyn – art. 15
Proposjonalitet – mål/middel
Informert – art 13 og 14
Samtykke – art. 4 (11)
Resosialisering
Anonymitet
Reservasjon – art. 22

GDPR vs. Nasjonal lovgivning

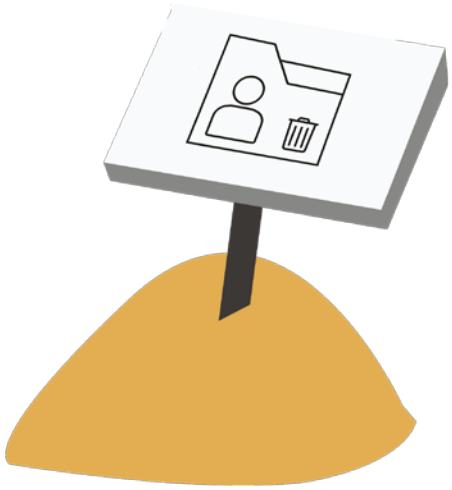
Nasjonal lovgivning vil **ikke** gå foran GDPR.

Nasjonal lovgivning må **tilpasses** GDPR,

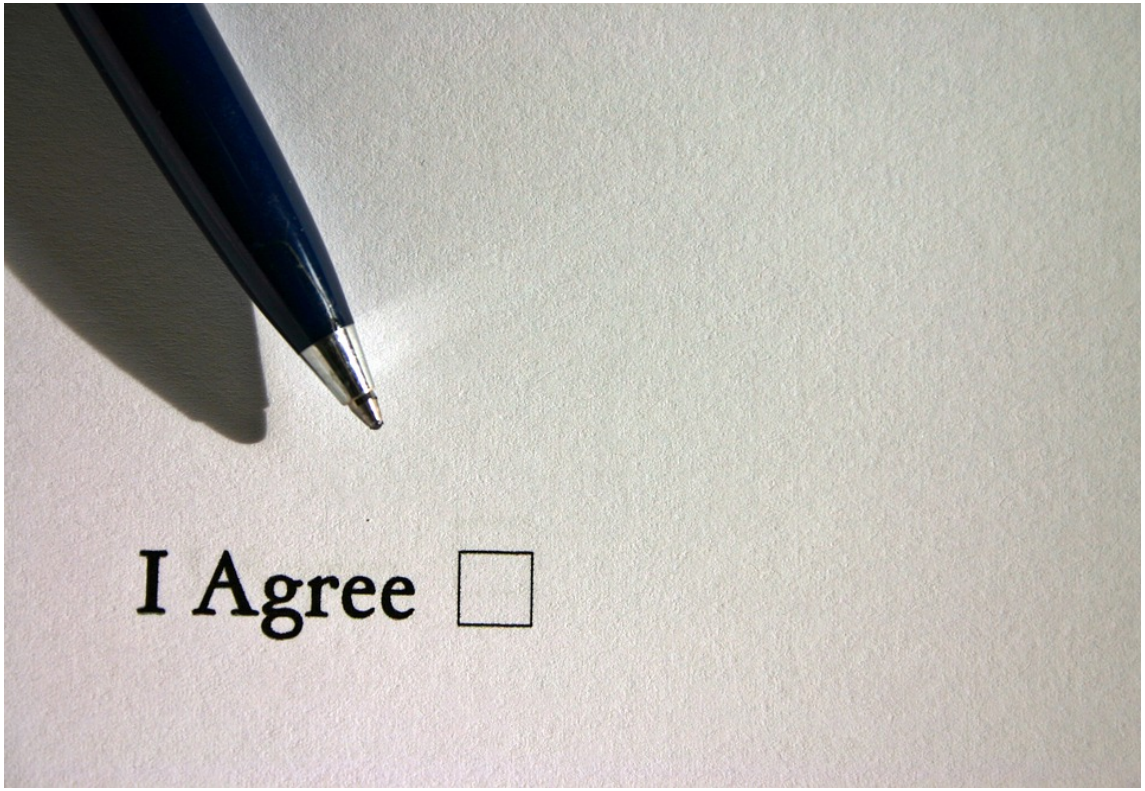
Bl.a ved å være i harmoni med GDPR kap. II om prinsippene.

Retten til dataportabilitet – art. 20

- Ny rettighet (som utfyller retten til innsyn)
- Gir den registrerte mulighet til å motta og gjenbruke sine data til egne formål og mellom tjenester
- Behandlingsansvarlig må kunne:
  - Gi ut personopplysninger til den registrerte
  - Overføre til ny behandlingsansvarlig – der det er teknisk mulig
- I et strukturert, allment brukt og maskinlesbart format
  - F.eks. ikke e-postdata som PDF
  - Det må være strukturert nok til at metadata beholdes, og at f.eks. e-post kan gjenbrukes i et nytt verktøy



Samtykke



Samtykke

POL	Direktivet	GDPR
• Frivillig	- frivillig	- frivillig
• Uttrykkelig	- spesifikk	- spesifikk
• Informert	- informert	- informert
		- utvetydigt

Med informert menes

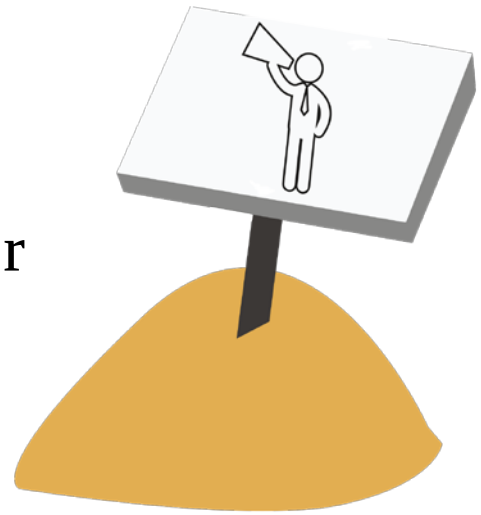
- Behandligsansvarliges identitet
- Formålet
- Tilbaketrekking av samtykke

Barns samtykke

- Prinsippet: Barn bør nyte særlig beskyttelse, jf. fortalen nr. 38
- Nettjenester rettet direkte mot barn - særskilte regler:
  - Fra og med oppfylt 16 år, kan barn samtykke.
  - Under 16 år:
    - Norge kan bestemme at barn mellom 13-16 år kan bruke disse tjenestene uten foreldrenes samtykke.
  - Den behandlingsansvarlig skal sørge for å unngå at aldersgrensen omgås:
    - Rimelige tiltak for å verifisere at den som har foreldreansvar for barnet har gitt sitt samtykke
    - Tjenestetilbyderen må som en del av dette vurdere hva som er teknisk mulig å få til.

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



Informasjonsplikt (1- HVA?)

- Den behandlingsansvarlige skal iverksette egnede tiltak for å ivareta personvernet:
  - informasjonsplikt når det samles inn opplysninger fra den registrerte (art. 13)
  - informasjonsplikt når det samles inn opplysninger fra andre enn den registrerte (art. 14)
  - opplyse om de registrertes rettigheter etter art. 15-22
  - underretting om sikkerhetsbrudd til de berørte, jf. art. 34

Sletting

Retting (popplyl § 27/ pvf art 16 + art 19)

- Opplysninger:
  - Uriktige
  - Ufullstendige, eller
  - Ikke er adgang til å behandle
- Varsling av tredje part:
  - *om mulig*, sørge for at feilen ikke får betydning for den registrerte, *f.eks. ved å* varsle

- Opplysninger:
  - Unøyaktige
- Varsling av tredje part:
  - Plikt dersom kravet er etterkommet
  - *Umulig/uforholdsmessig vanskelig*
  - Som en minimum, plikt til å oppgi identiteten til tredjepartsmottakere hvis den registrerte ber om det
- Når? uten ugrunnet opphold

Sletting etter anmodning (popplyl § 28 / pvf art 17)

- Opplysninger:
  - Sterk belastende
- Dersom dette ikke:
  - strider mot annen lov, og

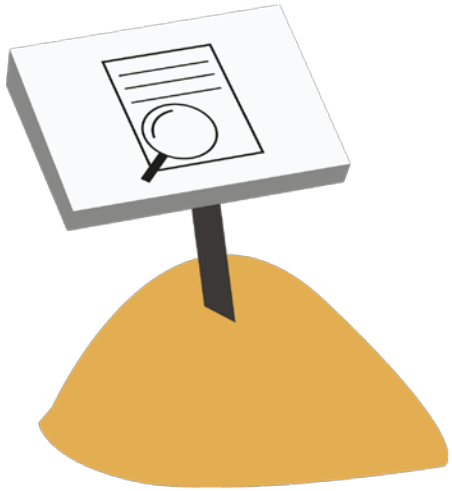
- Opplysninger:
  - Ikke nødvendige
  - Samtykket trekkes tilbake
  - Registrerte motsetter seg, og det ikke er legitime grunner
  - Ulovlig behandling

Underretning av tredjepart ved sletting art 17 + art 19

- Art 19 gjelder også sletting
  - Plikt dersom kravet er etterkommet
  - *Umulig/uforholdsmessig vanskelig*
  - Som en minimum, plikt til å oppgi identiteten til tredjepartsmottakere hvis den registrerte ber om det

Alle skal vurdere risiko og personvernkonsekvenser -

- I tillegg til en risikovurdering skal man utrede tiltak med stor personvernrisiko art. 35
- Ved høy risiko, som ikke kan begrenses, skal Datatilsynet involveres i forhåndsdrøftelser
- Forordningen stiller krav til vår behandlingstid
- Vi kan veilede eller forby behandlingen

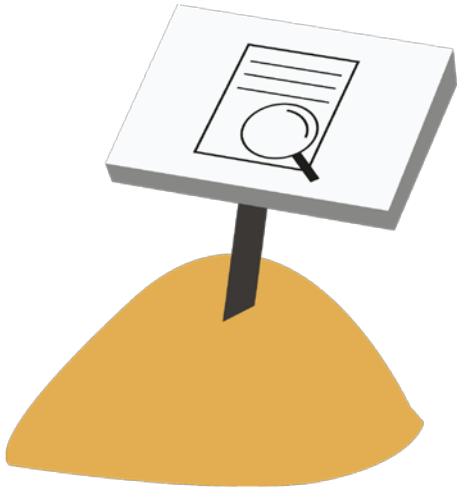


Eksempler på spørsmål ved kartlegging:

- ❖ Hvilke personopplysninger skal applikasjonen få tilgang til, samle inn eller overføre? Hvordan kan dette berøre brukerne?
- ❖ Dokumenter at innsamlingen har et legitimt formål, og i hvilken grad du er berettiget til å samle inn slike data.
- ❖ Hvilke følger kan det få for en bruker av applikasjonen dersom data skulle bli misbrukt?
- ❖ Hvor presist og hvor enkelt kan en spesifikk person eller enhet identifiseres basert på disse opplysningene?
- ❖ Hvor lenge skal personopplysningene lagres?
- ❖ Er applikasjonen rettet mot barn?
- ❖ Hvor lett er det for brukeren å slette personopplysningene eller brukerkonti?

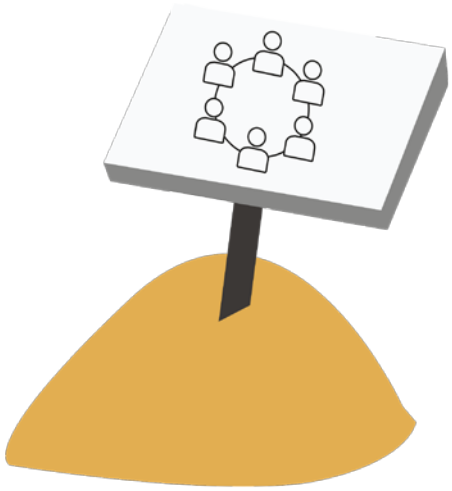
Forhåndsdrøftelser – Art. 36

- Artikkelen baserer seg på at det er gjennomført en DPIA (Data Protection Impact Assessment) og at det er høy risiko som ikke kan reduseres.
- Det stilles krav til dokumentasjon som skal sendes inn til oss
- Vi kan veilede eller forby behandlingen
- Artikkel 36 (5) kan relateres til dagens konsesjonsbehandling. Nasjonal rett kan kreve at behandlingsansvarlig skal drøfte og innhente forhåndstillatelse - behandlinger i allmenn interesse, herunder *social protection* og *public health*.



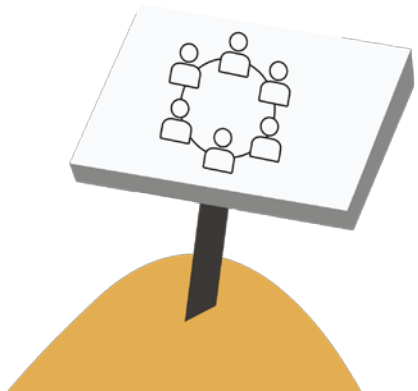
Atferdsnormer – art. 40

- Artikkelen er en utvidelse av dagens regelverk - § 42 pkt 6
- Datatilsynet skal oppmuntre til utarbeidelse av normer, for å sikre effektiv etterlevelse av forordningen, særlig mht konkrete karakteristikker av behandlinger i ulike sektorer og av særlige behov for mikro, små og mellomstore virksomheter.
- I artikkel 40 (2) nevnes det eksempler på hva som kan spesifiseres i en norm, som blant annet:
  - Rettferdig og åpen behandling, innsamling av personopplysninger, pseudonymisering, informasjon, varsling av avvik, overføring til tredjeland m.v.

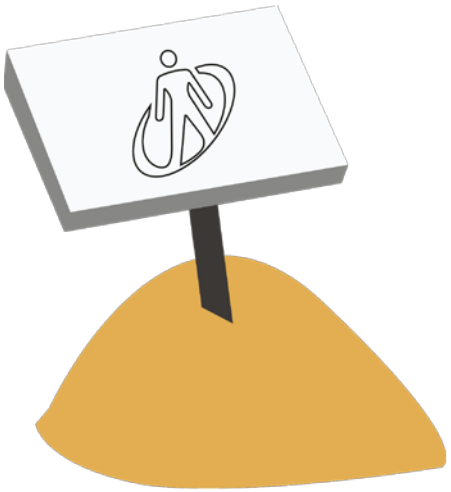


Atferdsnormer – art. 40

- Utkast, endringer eller utvidelser av normer sendes til Datatilsynet for godkjenning. Vi registrerer og offentliggjør.
- Dersom flere land berøres av normen er det en prosess hvor kompetent myndighet sender til EDPB, som gir sin uttalelse til kommisjonen, som kan beslutte å godkjenne allmenn gyldighet. Offentliggjøres av kommisjonen. EDPB har register med godkjente normer.
- Vi må få på plass rutiner for håndtere prosessen med å godkjenne normer.



Personvernombud – art. 37



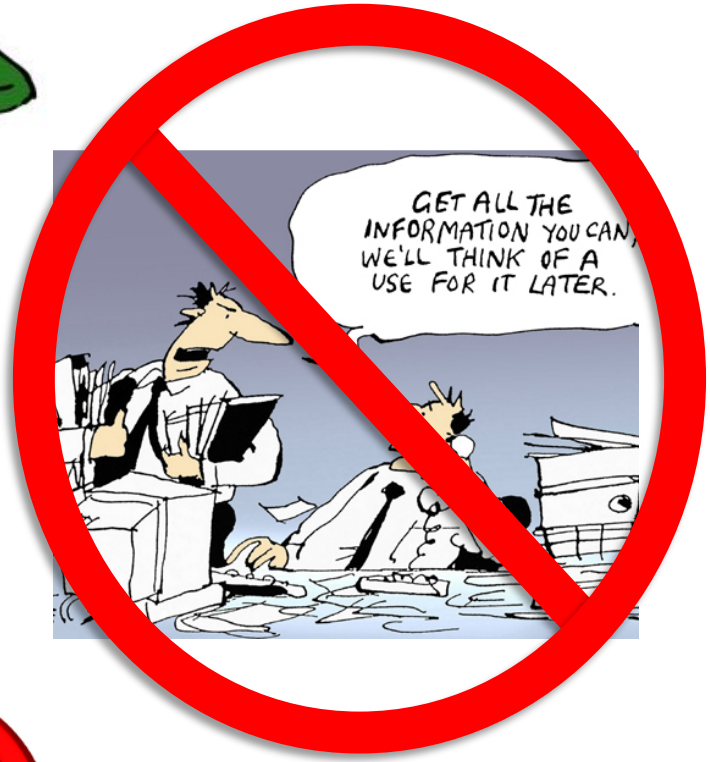
- Disse må ha ombud:
  - Alle offentlige virksomheter (unntatt domstoler)
  - Virksomheter som har som kjerneaktivitet å gjøre følgende i stor skala:
    - regelmessig og systematisk overvåke personer
    - behandle sensitive personopplysninger eller opplysninger om straffbare forhold

Strengere krav til personvernombudene

- Krav til kompetanse
- Skal involveres og rapportere til høyeste ledelsesnivå
- Ombudet skal ikke instrueres eller straffes
- Oppgavene omfatter å gi råd, overvåke etterlevelse og være kontaktpunkt

Innebygd personvern og personvern som standard – art. 25

- Tekniske og organisatoriske tiltak
  - F.eks. pseudonymisering
- Utformet for å ivareta personvernprinsipper
  - F.eks. minimalisering
- Det minst personverninngripende alternativet som standard:
  - mengde
  - omfang
  - lagringstid
  - tilgjengelighet



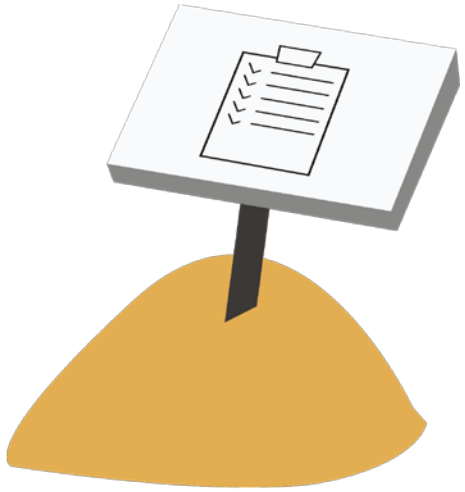
Alle skal bygge personvern i løsningene sine

Innebygd personvern:

- Nye krav til løsninger, tiltak og systemer
- Ta hensyn til personvern i alle utviklingsfaser av et system eller en løsning.
- Det er både kostnadsbesparende og mer effektivt enn å endre et ferdig system.
- Skal utarbeides på mest mulig personvernvennlig måte
- Den mest personvernvennlige innstilingen som standard

Oversikt over behandlingsaktiviteter – art. 30

- Kontaktinformasjon til behandlingsansvarlig
- Formål
- Kategorier av registrerte og personopplysninger
- Kategorier av mottakere
- Evt. overføringer til tredjeland eller internasjonale organisasjoner, og dokumentasjon på tilstrekkelig beskyttelse
- Slettefrister
- Sikkerhetstiltak



Databehandlere skal ha tilsvarende oversikt over det de gjør på vegne av ulike behandlingsansvarlige

Oversikt over behandlingsaktiviteter – art. 30

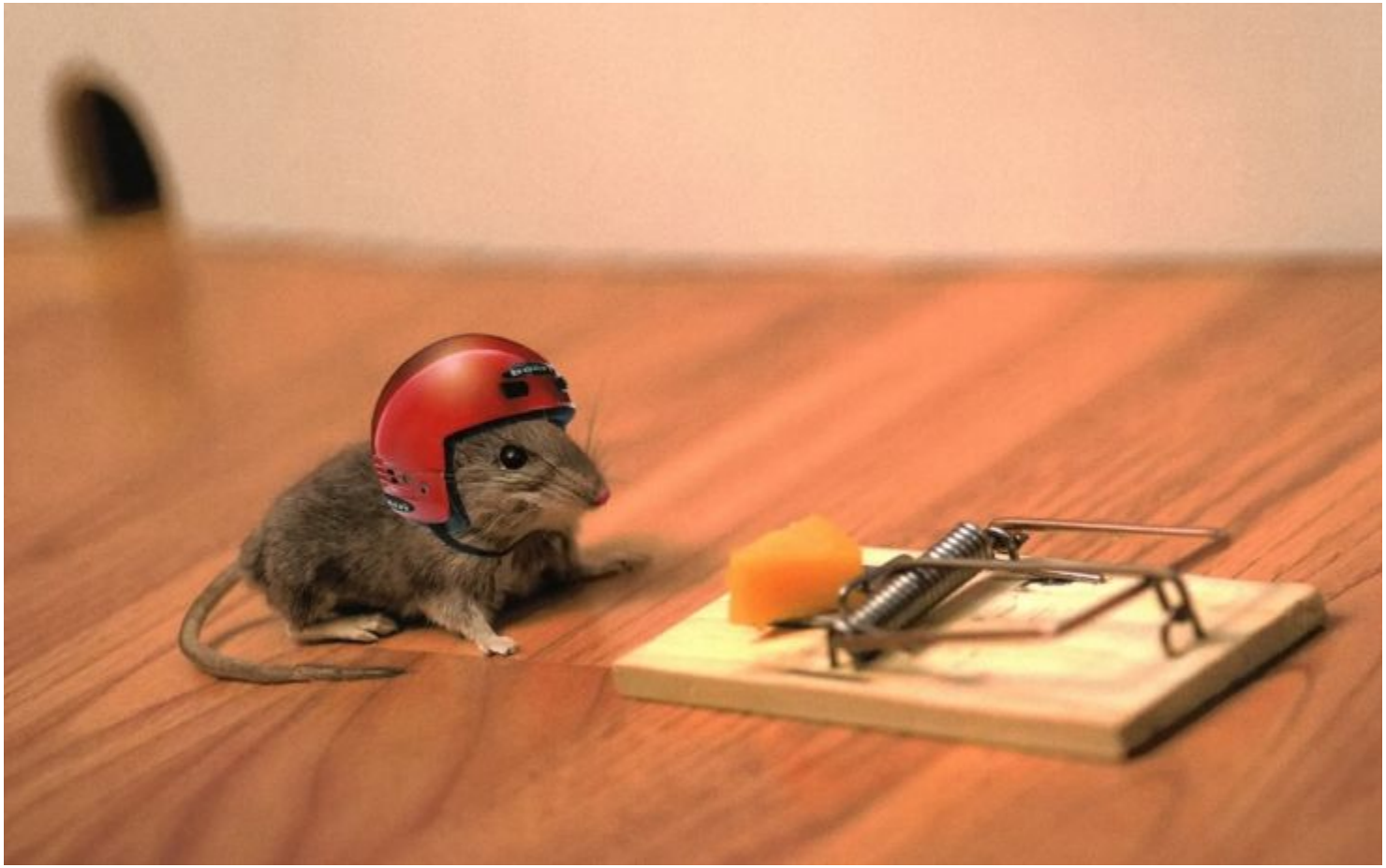
- Det finnes relaterte plikter i personopplysningsloven § 14, jf. forskriften § 3-1, og § 13, jf. forskriften § 2-4
- Artikkel 30 bygger på «ansvarlighetsprinsippet» i artikkel 5 (2). Meldeplikt utgår, men behandlingsansvarlig og databehandler må ha oversikt hos seg selv.
- Hva betyr artikkel 30 (5):

  «Forpliktelsene nevnt i nr. 1 og 2 får ikke anvendelse på et foretak eller en organisasjon med færre enn 250 ansatte, med mindre behandlingen det/den utfører, trolig vil medføre en risiko for de registrertes rettigheter og friheter, behandlingen ikke skjer leilighetsvis eller omfatter særlige kategorier av opplysninger som nevnt i artikkel 9 nr. 1 eller personopplysninger vedrørende straffedommer og straffbare forhold nevnt i artikkel 10.»

Informasjonssikkerhet

Sikkerhet ved behandling – art. 32

- Risikovurdering

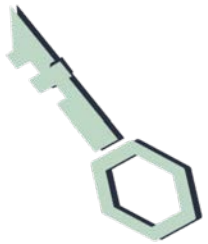


Sikkerhet ved behandling – art. 32

- 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
- Atferdsnormer 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

Avvik art. 33

Irenes private helseopplysninger lå åpent ute på nett: – Sjokkerende og ekkelt

En rekke dokumenter med sensitive personopplysninger fra Bodø kommune har ligget åpent og søkbart ute på nett. – Sjokkerende, sier Irene Olsen, etter at hennes private helseopplysninger ble lekket på nett.

Eksempler:

Politiske parti

Bruk av minnepenn

Tyveri av bærbar PC

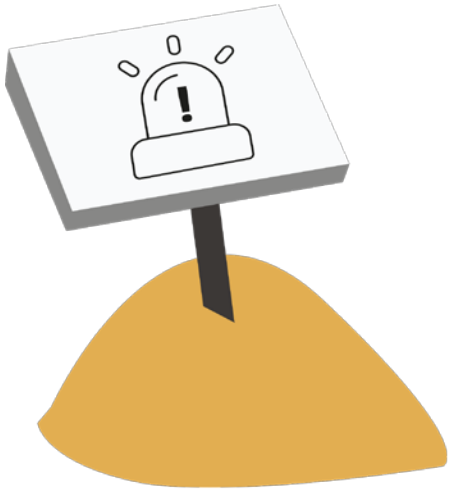
St. Olavs Hospital

Årdal kommune

Andebu kommune

Råde kommune

Avviksmeldinger – art. 33

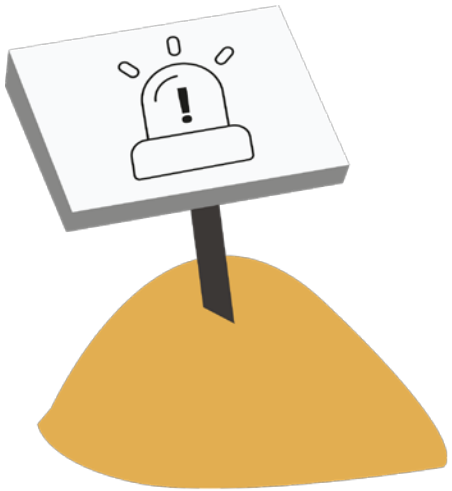


Sikkerhetsbrudd (art. 4 (12)):
«brudd på personopplysningssikkerheten» - er et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet

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

«uautorisert utlevering av personopplysninger som krever konfidensialitet»

Avviksmeldinger – til Datatilsynet - art. 33

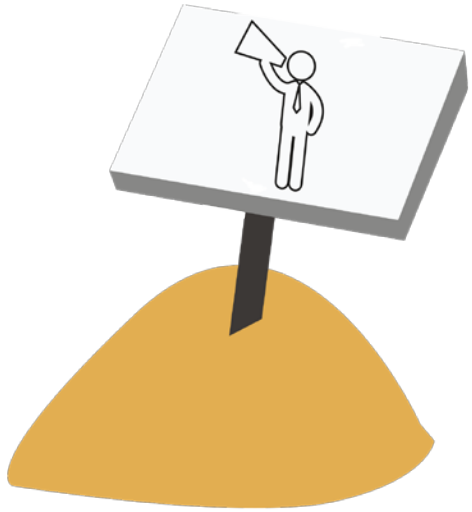


- Behandlingsansvarlig må melde avvik innen 72 timer. Kan meldes trinnvis.
- Databehandler melder til behandlingsansvarlig
- Stilles krav til innholdet i avviksmeldingen. Vårt skjema i Altinn tar høyde for dette.
- Finnes en uttalelse fra Artikkel 29-gruppen (2014) som skal oppdateres i løpet av året. Gjelder både artikkel 33 og 34.


-OG DE
INFORMERTE
IKKE
DATATILSYNET!

Informasjon til de berørte – art. 34

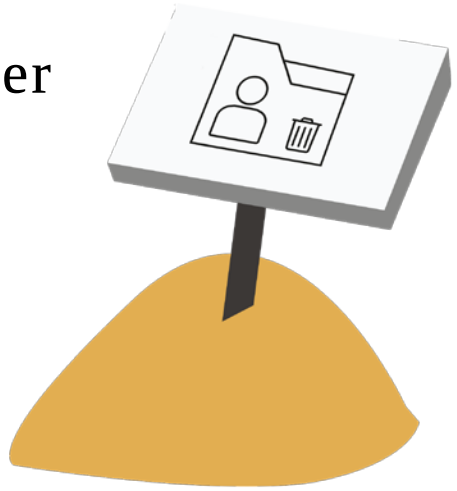
- Kravet finnes ikke i dagens regelverk, men ny praksis er gått opp med «GE-sakene» i Personvernnemnda (artikkel på datatilsynet.no)
- Berørte skal informeres så raskt som mulig, slik at de skal kunne foreta seg noe for å begrense skaden.



- 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



Når er dere compliant med GDPR

Strategier for etterlevelse av regelverket for å bli compliant

1. Sett dere inn i regelverket og få **oversikt** over hvilke personopplysninger dere behandler
2. Gjennomgå alle **personvernerklæringer**
3. Sørg for at dere kan oppfylle **de nye rettighetene** (dataportabilitet, retten til å si nei til profilering etc.)
4. Planlegg hvordan dere skal håndtere **innsynsbegjæringer, sletting av data** etc.
5. Gjennomgå **behandlingsgrunnlagene** dere benytter. Tilfredsstiller de GDPR?
6. Gjennomgå hvordan dere innhenter **samtykke**. Er det «frivillig» og kan det trekkes tilbake?
7. Ha god informasjonssikkerhet – **risikovurdering**
8. Hvilke **personvernkonsekvenser** er det
9. Rutiner for **avvikshåndtering**. Det blir krav om å rapportere alle avvik til Datatilsynet
10. Implementer personvern **i hjertet av alle nye prosjekt** (innebygd personvern + DPIA)
11. Skaff dere **personvernombud**
12. Lag **atferdsnormer**

Datatilsynet.no/forordning