Nye personvernregler fra mai 2018

Kristiansund 14. juni 2017

Knut B. Kaspersen - Datatilsynet

Datatilsynet

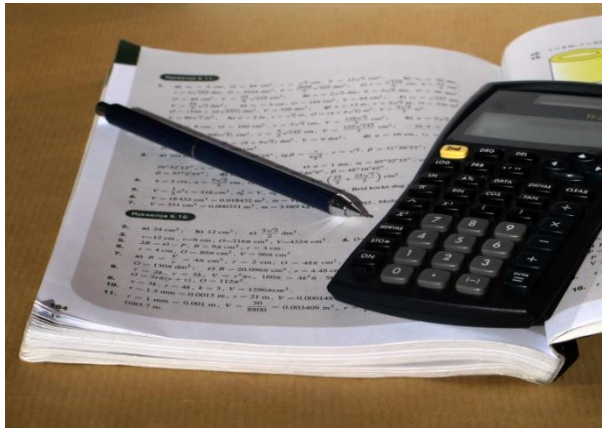
Personvern

Hva er det?

Personopplysninger – hva er det?

Peder Aas
2020 Lillevik

F.nr 180262 34997



Personopplysninger – hvor er de?

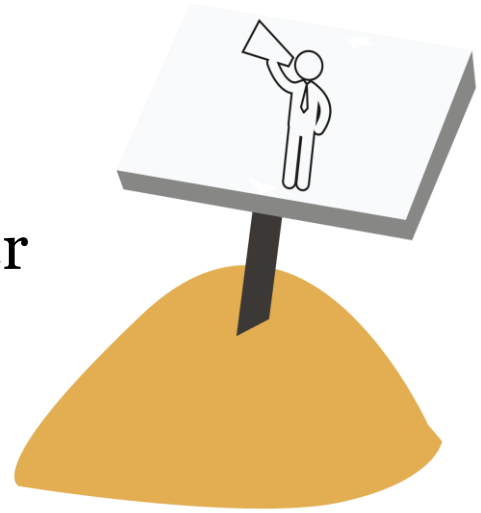

General
Data
Protection
Regulation

Viktig nytt i forordningen

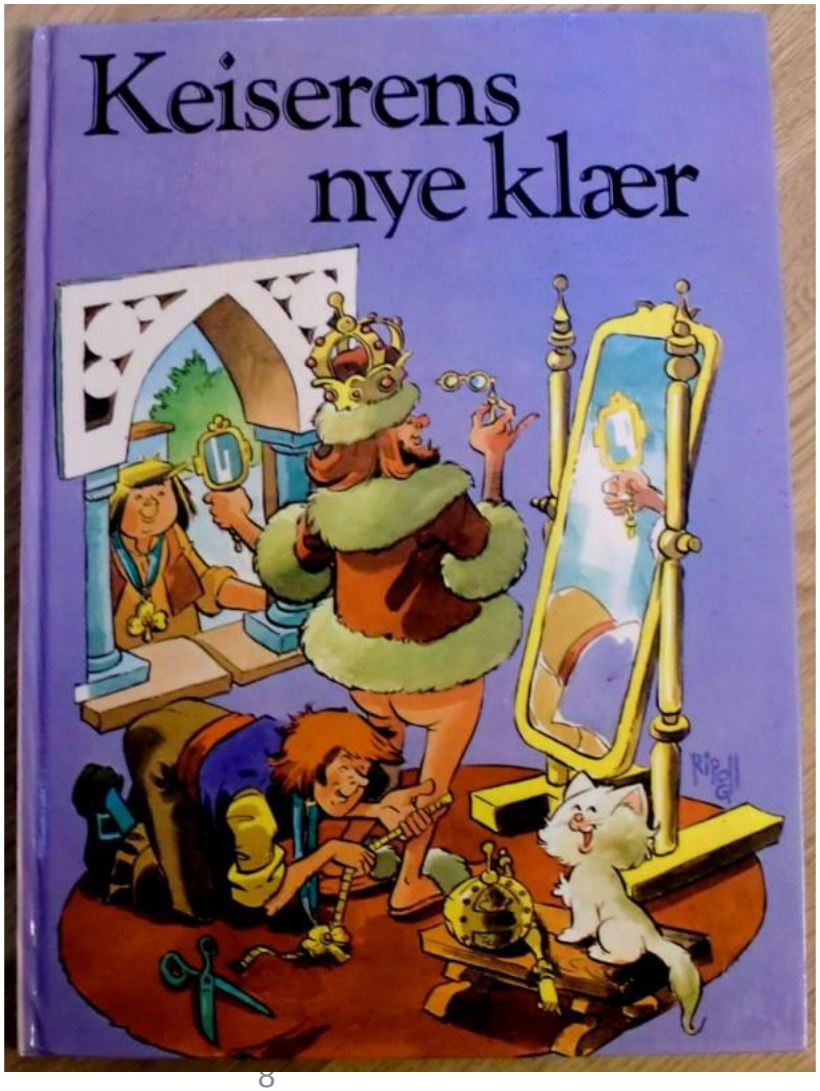
- Materielle krav i regelverket:
  - ✓ Innebygd personvern og personvern som standard innstilling
  - ✓ Vurdering av personvernkonsekvensene
  - ✓ Mer tydelige krav til informasjon og samtykke
  - ✓ Mye strengere sanksjoner
- Strategier for etterlevelse av regelverket:
  - ✓ Obligatorisk personvernombud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

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

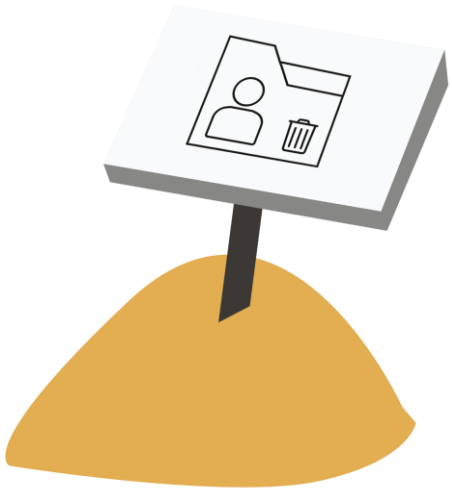


Noe nytt, eller . . . ?



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



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.

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

Informasjonsplikt (2- HVORDAN?)

- konsis, gjennomsiktig, forståelig og lett tilgjengelig form, i et klart og enkelt språk
- uten vederlag
  - med mindre anmodningene fra de registrerte er åpenbart grunnløse eller overdrevne, spesielt hvis de gjentar seg over en viss periode, jf. 12(5)

- NÅR: uten ugrunnet opphold og ikke senest enn en måned etter anmodningen er mottatt
  - kan forlenges med 2 måneder dersom nødvendig

- Dersom anmodningen er avslått, skal det informeres uten ugrunnet opphold og innen en måned om dette, og om muligheten til å inngi en klage til DT og innbringe saken for en rettsinstans.

Presiseringer

- Allmennheten har ikke et generelt rett til innsyn
  - «enhver som ber om det» (popplyl § 18)
- Den BA skal følge en bestemt fremgangsmåte når de gir informasjon ved innhenting av samtykke
  - «planlagte og systematiske tiltak» (popplyl § 14)
- Tidsfrister for å gi informasjon
  - «uten ugrunnet opphold og senest innen 30 dager» (popplyl § 16)
- Ny fremgangsmåte ved «åpenbart grunnløse eller overdrevne» anmodninger (art 12(5))
- Retten til å bli glemt (art 17)

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
- Ved tungtveiende personvernhensyn kan Datatilsynet bestemme sletting eller sperring

- 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
  - er forsvarlig …ressurser gjennomføringen av kravet forutsetter

- Opplysninger:
  - Ikke nødvendige
  - Samtykket trekkes tilbake
  - Registrerte motsetter seg..
  - Ulovlig behandling
  - Lovhjemmel
- Ingen direkte adgang til å ta kostnadene med i beregningen
- Ingen behov for intervensjon fra Datatilsynet

Underretning av tredjepart ved sletting art 17(2) + 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

- Nytt: plikt til å informere tredjepart som behandler data som er tilgjengeliggjort for allmenheten (art 17 (2))
  - *Rimelige tiltak*, tatt i betraktning tilgjengelig teknologi og gjennomføringskostnader
  - Kun plikt til å informere dem

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

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?

Minst to av følgende ti kriterier

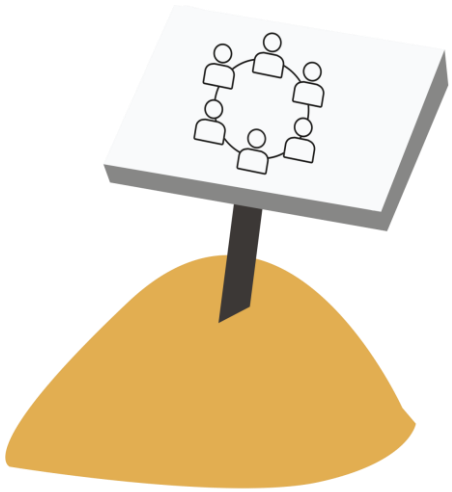
1. Evaluering eller poengvurdering *(scoring)*
2. Automatiserte avgjørelser
3. Systematisk overvåkning (*monitoring*)
4. Sensitive personopplysninger
5. Behandling av personopplysninger i stor skala
6. To eller flere datasett som sammenstilles
7. Personopplysninger om registrerte med særskilt beskyttelsesbehov
8. Ny teknologi eller bruk av eksisterende teknologi til nye formål
9. Overføring til utlandet
10. Konteksten begrenser muligheten for de registrerte til å utøve rettigheter

Forhåndsdrøftelser – Art. 36

- Artikkelen baserer seg på at det er gjennomført en DPIA og at det er høy risiko som ikke kan reduseres.
- Det stilles krav til dokumentasjon som skal sendes inn til oss
- Forordningen stiller krav til vår behandlingstid
  - 8 uker, kan forlenges innen én mnd (må begrunnes) til ytterligere 6 uker
- 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.

Mange virksomheter må opprette personvernombud

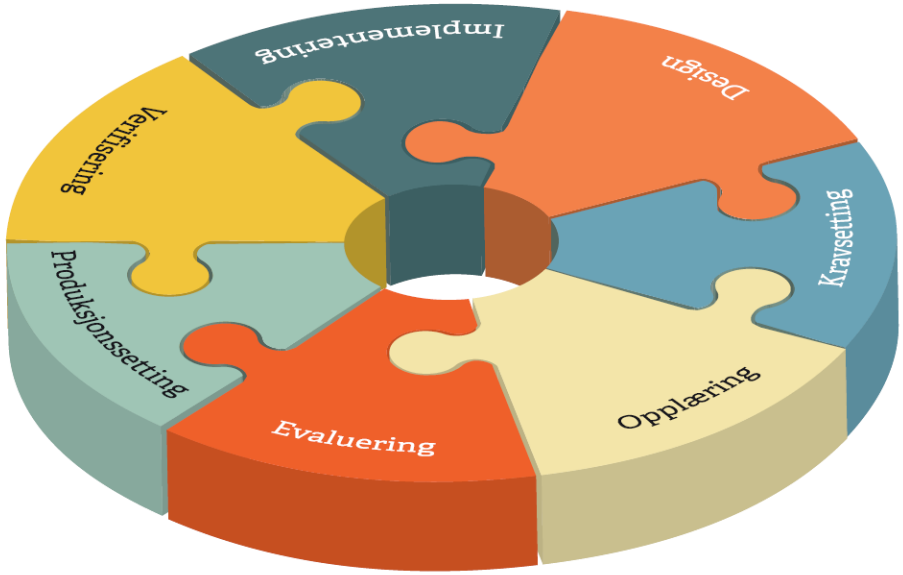
- Disse må ha ombud:
  - Alle offentlige virksomheter (unntatt domstoler)
  - Virksomheter som har som kjerneaktivitet å gjøre følgende i stor skala:
    - regelmessig og systematisk overvåke personer
    - behandle sensitive personopplysninger eller opplysninger om straffbare forhold

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

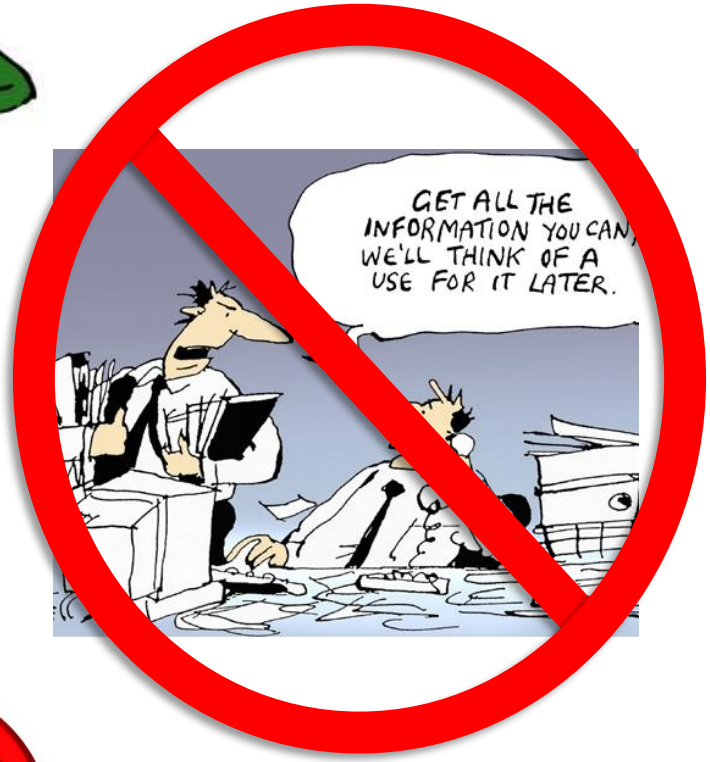
Innebygd personvern og personvern som standard – art. 25

- Ny plikt for behandlingsansvarlige
- Knyttes til internkontrollpliktene i art. 24
- Sertifisering kan bli brukt som element for å vise etterlevelse



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



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.»

Sikkerhet ved behandling – art. 32

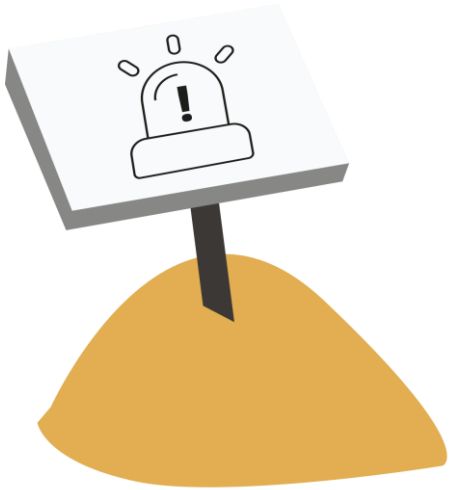
- Risikovurdering
- Sikkerhetstiltak
  - Pseudonymisering og kryptering av personopplysninger
  - Sikre vedvarende K, I, T og robusthet
  - Gjenoppretting av tilgjengelighet og tilganger ved hendelser
  - Jevnlig testing, vurdering og evaluering
- Bransjenormer eller godkjent sertifiseringsordning
  - 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

Avviksmeldinger – art. 33

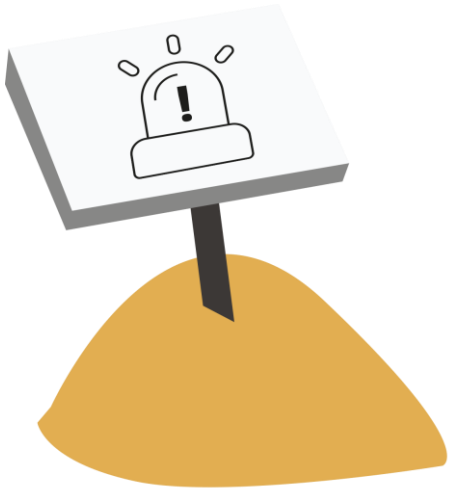


Sikkerhetsbrudd (art. 4 (12)):
«brudd på personopplysningssikkerheten» - er et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet

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.

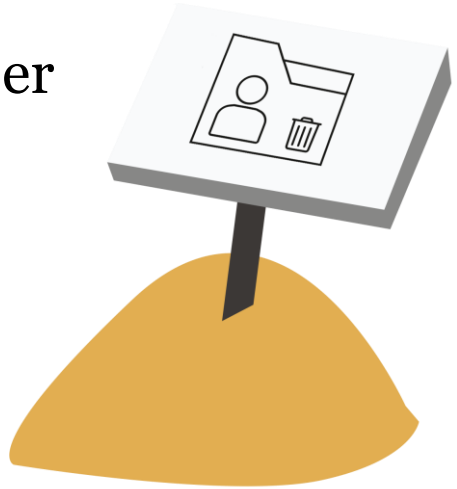
Informasjon til de berørte – art. 34

- 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 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



Datatilsynets forventninger til dere…

1. Vet dere hvem «deres registrerte» er?
2. Vet dere noe om hvordan de verdsetter sitt personvern?
3. Vet dere hvilke opplysninger dere har om de registrerte og hvor disse opplysningene kommer fra ?
4. Vet dere hvorfor dere trenger akkurat disse opplysningene om de registrerte? Eventuelt om dere kan gjennomføre oppgavene med færre opplysninger?
5. Vet dere hvem i deres organisasjon som beslutter om opplysninger skal slettes/rettes og hvem som teknisk sett kan gjennomføre endringene? Eventuelt hvor lang tid det tar?
6. Vet dere hvor dere finner informasjon om deres internkontrollsystem og rutiner for informasjonssikkerhet og hvordan dette kan hjelpe dere i arbeidshverdagen?

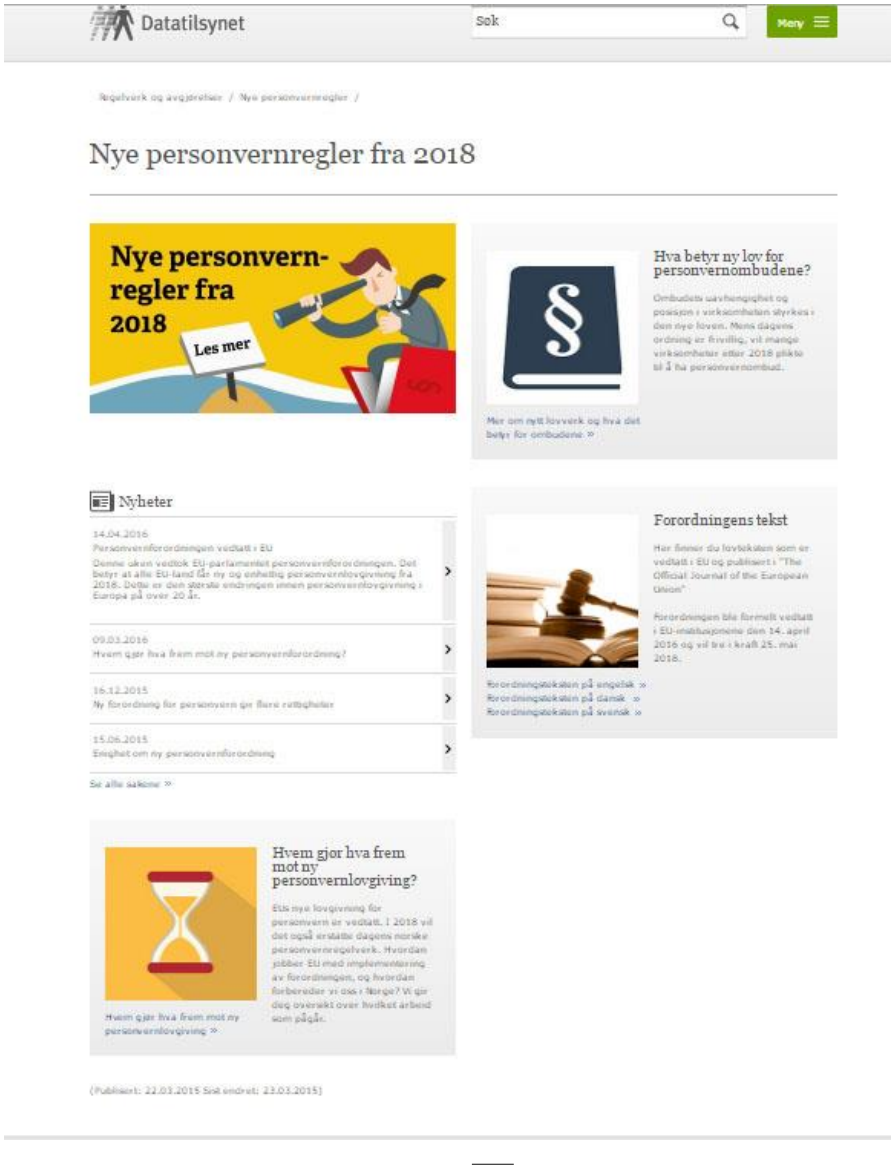
Hva bør alle virksomheter gjøre nå?

- 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

Sanksjoner – Overtredelsesgebyr – art. 83

- Behandligsansvarliges (også databehandlers) **forpliktelser** i FO
  - 10 mill. EUR (eller 2 % av årlig globale omsetning for en virksomhet)
- Overtredelse av **grunnprinsippene** (inkl. samtykke)
  - 20 mill. EUR (4 %)
- Overtredelse av **påbud** fra Datatilsynet
  20 mill. EUR (4 %)
- Usikkerhet for **offentlige myndigheter**
  - Avgjøres nasjonalt

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 person-opplysninger

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

2

Systemer, tjenester og løsninger som oppfyller prinsippene om innebygd personvern

Velg den mest personvernvennlige 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

Tilfredsstillende 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 prose-dyrer 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 avvikshåndtering

Forordningen stiller strengere krav til avvikshåndtering 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