
HORDALAND FYLKESKOMMUNE

# Forum for Kontroll og Tilsyn 27. mars 2019 Sekretariatskonferanse

Personvernombud Marianne Seim

# Personvern


Ny personvernlovgivning:

Personopplysningsloven av 20. juli 2018.
EUs personvernforordning (GDPR) «gjelder som lov» (§ 1).

Ny lovgivning stiller krav til hvordan virksomheter håndterer personopplysninger.

Særlovgivning:

pasientjournalloven
helseregisterloven
arbeidsmiljøloven
ulike taushetspliktregler i annen lovgivning
mm.

# Personvernombud

- Nøkkeloppgaver: Informere og øke kompetansen om personvern i virksomheten, gi råd (rådgiver for virksomheten og dens ansatte), kontrollere etterlevelse av regelverket, kontaktpunkt for de registrerte og tilsynsmyndighetene.
- Uavhengig.
- Organisert faglig i direkte linje til fylkesrådmannen.
- Utarbeid en instruks / mandat for rollen – behovet for det.
- Orientere meg i en stor og kompleks virksomhet.
- Gjøre prioriteringer der hvor personvernrisikoen er høyest (barn / unge, elever og pasienter).

# Personvernombud fortsetter

- Plikt til å ha personvernombud?

- Personvernforordningen artikkel 37 nr. 1 skal det utpekes personvernombud dersom visse vilkår foreligger «..behandlingen utføres av en offentlig myndighet eller et offentlig organ».
- Hva som er «offentlig myndighet / organ» finnes det liten veiledning i forarbeidene på, men det beror på en konkret vurdering (hva er kjernevirksomhet og omfattet av forvaltningsloven, enkeltvedtak /beslutninger /utøves offentlig myndighet, omfanget av behandling av personopplysninger).
- Juridisk vurdering for Norges Kommunerevisorforbund (NKRF).
- Interkommunale selskaper / samarbeid og samvirkeforetak ikke er omfattet av kravet til å utnevne personvernombud, vektlagt at behandling av personopplysninger ikke er en del av kjerneoppgavene VS eget Kontrollutvalg.
- Uansett: Må vurderes konkret om det likevel er hensiktsmessig å ha et personvernombud.
- Virkningen av å ikke ha et personvernombud?
- Personvernombud eller ei, personopplysningsloven og personvernforordningen skal likevel følges og etterleves.

# Personvern

Sentrale begreper i personvernlovgivningen:

«Personopplysning»: «Enhver opplysning om en identifisert eller identifiserbar fysisk person, som direkte eller indirekte kan identifiseres ved hjelp av identifikatorer (navn, fødselsnummer, id.nummer osv.).»

«Særlige kategorier av personopplysninger»: «Rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, overbevisning eller fagforeningsmedlemskap, genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.»

«Den registrerte»: «Den fysiske personen som personopplysningene gjelder.»

«Behandling»: «Enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger.»

«Behandlingsansvarlig»: «En fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen og hvilke midler som skal benyttes.»

«Databehandler»: «En fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige.»

# Personvern

Nye regler gir nye rettigheter for den registrerte:

Krav på informasjon og strengere krav til å bruke samtykke

Innsyn i egne opplysninger

Rett til korrigering / sletting av opplysningene

Begrensning av behandling av personopplysninger

Innsigelse mot behandling av personopplysninger

Dataportabilitet

Varsling av den registrerte ved sikkerhetsbrudd / avvik

Protokollsystem for personopplysningene

# Personvern

Nye regler gir nye plikter for behandlingsansvarlige (virksomheten):

Protokollsystem som dokumenterer ansvaret for personopplysningene / behandlingsaktivitetene.

Foreta risikovurderinger og personvernkonsekvenser (DPIA).

Informasjonsplikt (formidles typisk via personvernerklæringer på relevante nettsider).

Avvikshåndtering og informasjon til den registrerte.

Ha kontroll på leverandørsiden (krav til databehandleravtaler).

# Personvern fortsettelse plikter..

Innebygd personvern (eksempelvis tilgangsstyring, sletterutiner, sikre soner mm).

Krav om personvernombud.

Melde- og konsesjonsplikten er bortfalt.

Kunne oppfylle den registrertes rettigheter (innsyn, korrigering, sletting, dataportabilitet, krav på informasjon osv) og dokumentere etterlevelse.

- Strengere sanksjoner (20 M Euro / 4 % av årlig omsetting) ved brudd på reglene.

# Personvern

Personvernprinsippene

- Lovlighet; Rettslig grunnlag

- Rettferdighet; Forholdsmessighet mellom behandlingen og formålet

- Gjennomsiktighet: Informasjonsplikter og innsynsrettigheter

- Formålsbegrensning; Spesifikke, uttrykkelig angitte og berettigede, forbud mot uforenelige formål

- Dataminimering; Opplysningene skal være adekvate, relevante og nødvendige for formålet

- Riktighet; Opplysningene skal være korrekte og oppdaterte

- Lagringsbegrensning; Opplysningene skal anonymiseres eller slettes når formålet er oppnådd (unntak arkiv /bokføringsplikt og forskningsformål el.)

- Integritet og fortrolighet; Tilstrekkelig informasjonssikkerhet (hvem har tilgang og hvem deles opplysningene med)

*Ansvarlig; Den behandlingsansvarlige er ansvarlig for og skal kunne dokumentere etterlevelse.*

# Overordnet om innholdet i et internkontrollsystem

Økte dokumentasjonskrav etter GDPR:

- Etterlevelse og dokumentere etterlevelse av regelverket og personvernprinsippene.
- Konsekvensutredning dersom høy personvernrisiko (DPIA / sikre at personvernet til de registrerte i løsningen ivaretas). Forordningen artikkel 35 angir når det er en plikt å gjennomføre en slik personvernkonsekvensanalyse (DPIA).
- Sikre innebygd personvern (mye et IKT spørsmål, bla. tilganger, dataminimering, automatisk sletting osv).
- Vedlikeholde oversikten over behandlinger (behandlingsprotokollene).
- Utarbeide og vedlikeholde nødvendig dokumentasjon, rutiner / prosedyrer, policy, interne regler.

# Overordnet om innholdet i et internkontrollsystem

## Styrende dokumenter:

- Hva er rammeverket for vår behandling av personopplysninger?

- Eks. overordnede prinsipper og retningslinjer/policy, behandlingsprotokoll, klargjøring av roller og ansvar, personvernerklæring, innebygd personvern, risikovurderinger.

## Gjennomførende dokumenter:

- Hvordan gjør vi det?

- Eks. Rutiner for innsyn, sletting, korrigering, innsigelse mot behandling, begrenset behandling, dataportabilitet, personvernerklæringer, rutiner for innsyn i ansattes e-post, bruk av kameraovervåking, mal for databehandleravtale, rutiner for bruk av samtykke / samtykkeskjema, avvik, databehandleravtaler, risikovurdering/DPIA, overføring ut av EU/EØS mv.

## Kontrollerende dokumenter:

- Hva følger vi opp og sjekker?

Eks. gjennomføring av revisjoner (internt/eksternt), rapportering, sjekklister, årshjul, avvikshåndtering.

# Overordnet om innholdet i et internkontrollsystem

Suksesskriterier for internkontroll:

- Forankring hos ledelsen.
- Kompetanseheving / informasjonstiltak / opplæring av nøkkelressurser.
- Innebygd personvern (bygge personvernet inn i løsningene og arbeidsrutinene).
- God dialog med Datatilsynet.
- Tilpasse internkontrollen til vår virksomhetsstruktur.

# Protokoll etter forordningen artikkel 30 (styrende dokumentasjon i internkontrollen)

- Virksomhetene har mange personopplysninger, ansatte / elever / barnehagebarn / pasienter ol.
- Opplysningene finne i mange systemer, både internt og hos leverandører.
- Hvilken kartlegging er best? Med utgangspunkt i de aktuelle systemene eller med utgangspunkt i prosesser (for tilsatte: rekruttering / under ansettelse / avslutning av arbeidsforhold?
- «Kjekt å ha mentalitet» contra GDPR krav (behandlingsgrunnlag, formål, dataminimering, sletting, personvernkonsekvenser).
- HFK har valgt prosess perspektivet i vår kartlegging.
- Behandlingsansvarlig i sekretariatene er leder / kontrollsjef.

Protokollen skal:

Minst inneholde det som er angitt i forordningen artikkel 30.

Være skriftlig (elektronisk).

Kartleggingen må klargjøre både behandlingsformål og hvilke applikasjoner som benyttes.

Hvorfor er kartleggingen viktig?

- Oppfyller vår plikt til protokoll etter artikkel 30.
- Gjør det enklere å identifisere «gap» som avdekkes ifm. arbeidet med protokollen og som må håndteres.
- Gir oss totaloversikt over hvor opplysningene befinner seg, gir oss oversikt over sårbare områder for personopplysningene, om vi har rettslig hjemmel til å behandle opplysningene og til hvilket formål, samler vi inn for mye informasjon enn formålet tilsier, deler vi opplysningene med noen evt. hvem, overfører vi opplysningene til noen evt. til hvem og hvor, kan vi sette inn noen tiltak som reduserer risiko og personvernkonsekvenser, er det behov for databehandleravtale osv.

## Personvernerklæring etter forordningen artikkel 13 og 14 (styrende dokumentasjon i internkontrollen)

- Plikt til å informere om de behandlinger vi gjør av personopplysninger jf. protokollene og jf. retten til informasjon for den registrerte og prinsipp om gjennomsiktighet.
- Krav til informasjonen som gis (må sette den registrerte i stand til å forstå hva vi gjør).
- Kan typisk formidles gjennom relevante nettsider (typisk skolens nettside, helsesøsters nettside).

## Databehandleravtale etter forordningen artikkel 28 og 29 (gjennomførende dokumentasjon i internkontrollen)

- Plikt til å bruke leverandører som gir tilstrekkelige garantier som sikrer at behandlingen oppfyller kravene i forordningen og vern av den registrertes rettigheter og friheter.

- Hvordan sikrer vi det?
- Konkretisering av personvernkrav i kravsspesifikasjonen når innkjøp skal gjøres.
- Når tjenesteavtale er inngått – vurdere behov for databehandleravtale:
- Behandler leverandør (databehandler) personopplysninger «på vegne av» HFK (behandlingsansvarlig)? Er taushetserklæring tilstrekkelig?
- Gjennom god dialog med leverandør og bruk av databehandleravtale vi kan sikre forsvarlig behandling av personopplysningene.

# Databehandleravtale etter forordningen artikkel 28 og 29 forts.

- HFK har egen databehandleravtalemal som kan brukes, men leverandør ønsker også sine brukt.
- Vurder innholdet i databehandleravtalen.
- Juridiske spørsmål; Bruk av underleverandører og overføring til tredjestater.
- Internkontroll og oppfølging av avtalene.

# Sikkerhetsbrudd / avvik etter forordningen artikkel 33 og 34 (kontrollerende dokumentasjon i internkontrollen)

- Hva er et sikkerhetsbrudd?

  Forordningen Artikkel 4 (12) «*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*»

*«utilsiktet eller ulovlig»* – det er tilstrekkelig at det foreligger brudd på virksomhetens sikkerhetstiltak.
Ikke krav om skyld – omfatter også rene uhell.
Uavhengig av hvilke opplysninger som er berørt.

- Meldeplikt til Datatilsynet (Artikkel 33), evt. Databehandler (Artikkel 33) og underretning til den / de registrerte (Artikkel 34) – Men noen unntak.

- Kort frist til Datatilsynet – senest innen 72 timer etter at brudd er oppdaget. Etter det må oversittet frist begrunnes for tilsynet.

- Etabler klare interne rutiner for hvem som har ansvar for hva og hvordan når sikkerhetsbrudd blir oppdaget. Tilsvarende avklar hvem som har tilgang til å melde til Datatilsynet. Det blir lett hektisk når sikkerhetsbruddet foreligger!

# Personvern

- Hvorfor bruke tid på å skape en virksomhet som fungerer i lys av GDPR?

- Persondata er viktige verdier som vi er lovpålagt å ha kontroll på og beskytte.
- Tillitsforholdet til borgerne og samfunnet rundt oss. Omdømme og integritet. Tilliten til at vi kan forvalte våre verdier og tjenester på en trygg og fornuftig måte.
- GDPR handler enkelt oppsummert om organisasjonens kvalitetssystem og håndtering. Vi må forstå hvordan og hvilke data vi samler inn og hvordan vi beskytter og håndterer disse og se løsninger ved digitalisering og teknologi.
- En rekke tiltak på ledelses/organisasjon/prosess, IT/IKT, leverandør, juridisk, individuelt og kollektivt hos ansatte - nivå mm må tas på alvor om vi skal lykkes. GDPR er derfor et virksomhetsansvar.
- Vi må skape en virksomhet som har en kultur for å håndtere persondata på en god måte – dette må bla. skje gjennom kompetanseheving- og holdningsendring hos ledere og ansatte og opplæring av nøkkelpersoner.

# Min erfaring fra GDPR arbeidet så langt

**Internt:**

- Må ha intern forankring for arbeidet med personvern for å lykkes.
- Digitalisering et nødvendig premiss for å lykkes med personvern.
- Fullmakts- og ansvarslinjer må på plass (hvem gjør hva?).
- Rutiner / maler / policy må utarbeides og implementeres / kvalitetssystem.
- Varierende GDPR modenhet i virksomheten. Vi har valgt å opprette personvernkoordinatorer i hver avdeling som sammen med leder har ansvar på området.
- Kompetanseheving for alle tilsatte og spesielt for de som har fullmakt og ansvar.
- Vi må øke fokuset på hvordan vi håndterer og deler personopplysninger.

**Leverandører:**

- Leverandørsiden må vi ha kontroll på (databehandlaravtaler og internkontroll), varierende GDPR modenhet også her.

**Prioritering contra risikoavveining:**

- Veien må også bli til mens vi går – det tar tid å bygge nye system og endre kultur.
- Erkjennelse. Vi rekker ikke alt samtidig: Hva skal prioriteres først? Hvilken risiko ligger i valgte prioriteringer? (faren for overtredelsesgebyr og omdømmemessige konsekvenser).