Sykehuset i Vestfold | HELSE SØR-ØST

Saksframlegg til styret

Møtedato: 28.5.2018

Sak nr.: 036/2018
Sakstype: Orienteringssak

Orientering om implementering av ny personvernlovgivning i SiV
Saksbehandler: Stein Kinserdal, Ida Mollerud

Trykte vedlegg (integrert i dokumentet):

1. Definisjoner
2. Datatilsynets punktliste til ny forordning

Hensikten med saken:
Hensikten med saken er å orientere styret om sykehusets implementering av ny personvernlovgivning. EUs forordning for personvern[1] blir etter planen norsk lov i løpet av juli 2018.

Forslag til vedtak

1. Saken tas til orientering
2. Administrerende direktør bes ha spesiell oppmerksomhet rettet mot oppfølging og praktisk implementering av endringer i fht. eksisterende lovgivning.

Tønsberg 28.5.2018

Stein Kinserdal
Adm. direktør

[1] General Data Protection Regulation – forordning (EU) nr. 2016/679

Faktagrunnlag:
EU har vedtatt en ny forordning (GDPR – General Data Protection Regulation) om behandling av personopplysninger. Justisdepartementet sendte på bakgrunn av dette et forslag til ny personopplysningslov på høring høsten 2017. I slutten av mars 2018 ble det endelige lovforslaget lagt fram. De nuye reglene skulle opprinnelig gjelde fra 25. mai 2018, mwn gjennomføringen er nå utsatt til minimum 1. juli 2018.

Forordningen gjennomføres i norsk rett ved at teksten i forordningen gjøres gjeldende i sin helhet vd en henvisningsbestemmelse i loven. De praktiske konsekvensene for virksomhetene er omfattende ved at de skal tilpasse interne systemer og rutiner til det nye regelverket.

Lovforslaget viderefører hovedprinsippene i den gjeldende personopplysningsloven, men reglene endres blant annet på følgende områder:

- De registrertes rettigheter er styrket på flerre punkter
- Mer åpenhet rundt innsamling og bruk av personopplysninger. Den som ber om samtykke til å bruke opplysningene skal gi klar og tydelig informasjon om hvordan personopplysningene skal brukes
- Bruk av personopplysninger skal begrunnes og begrenses. Det vil ikke være lov å samle inn eller lagre personopplysninger man ikke trenger. Opplysninger som det ikke lenger er behov for, skal slettes
- Det innføres en rett til å ta med se personopplysninger fra en virksomhet til en annen
- Den enkelte får rett til å protestere mot behandling av sine personopplysninger
- Den enkelte kan slippe at det blir truffet viktige avgjørelser om han eller henne basert på en helautomatisert behandling av personopplysninger

Det innføres plikt til å ha personvernrådgiver for offentlige myndigheter og for private virksomheter.

Dagens melde- og konsesjonsplikt bortfaller, men erstattes av en plikt til konsekvensutredning

Det vil bli adgang til å ilegge betydelig høyere gebyr ved overtredelse av reglene. Det åpnes for å gi overtredelsesgebyr på inntil fire prosent av virksomhetens årsomsetting, maksimalt 20 mill. Euro).

Innbyggerne skal ha tillit til at personopplysninger som SiV mottar blir behandlet og lagret på en trygg og sikker måte. Helse Sør-Øst RHF har gjennom oppdrag og bestilling (OBD) for 2017 og 2018 gitt foretaket i oppdrag å holde seg orientert om arbeidet med ny personvernforordning (GDPR) og gjøre nødvendige forberedelser for innføringen. Sykehuset arbeider over et bredt spekter for å sikre etterlevelse av krav i henhold til ny personvernlovgivning.

Krav til behandling av personopplysninger i sykehus:

Frem til 1978 hadde Norge ingen generell personopplysningslov. Sykehuset behandlet personopplysninger etter sykehusloven av 1969, legeloven av 1927, sykepleierloven av 1960 m.fl. Lovene hadde bestemmelser om taushetsplikt. I tillegg forholdt sykehusene seg til internasjonale erklæringer og konvensjoner; Menneskerettighetserklæringen (FN 1948), Den europeiske menneskerettighetskonvensjon (EMK 1950), Barnekonvensjonen (FN 1989) m. fl. I tillegg til særlover som gjelder ansatte og publikum, eksempelvis arbeidsmiljøloven og arkivloven.

I 1978 fikk Norge personregisterloven. I 2001 ble den avløst av gjeldende personopplysningslov med forskrift (gjennomfører EUs personverndirektiv 95/46/EU). I 2014 vedtok Stortinget å styrke vernet om den personlige integritet, ved å ta bestemmelsen om personvern inn i Grunnloven (ny § 102).

Personopplysningsloven er generell og har som formål å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger. Loven skal bidra til at personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger.

Bestemmelsene i loven gjelder for behandling av personopplysninger om ikke annet følger av en særskilt lov som regulerer behandlingsmåten. For sykehuset gjelder et stort antall særlover som regulerer behandling av pasient-, ansatt- og publikumopplysninger.

Nye personvernregler 2018:
EUs forordning for personvern blir norsk lov i løpet av 2018. Den erstatter EUs personverndirektiv fra 1995. Forordningen gjøres gjeldende som norsk rett «ord for ord», gjennom en henvisningsbestemmelse i ny personopplysningslov. Den nye personopplysningsloven vil tidligst bli satt i kraft i juli i år.

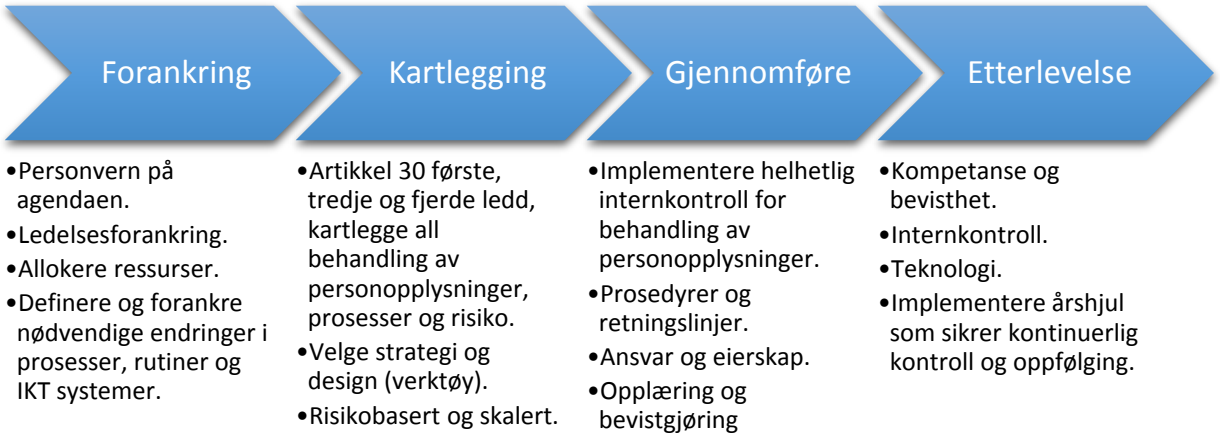
Forordningen oppstiller et omfattende generelt personopplysningsregelverk, herunder de grunnleggende prinsippene og vilkårene for å behandle personopplysninger, rettigheter for enkeltpersoner, plikter for behandlingsansvarlige og databehandlere, overføring av personopplysninger over landegrensene og regler om tilsyn og sanksjoner. Det legges vekt på ansvarlighet og internkontroll hos virksomheten fremfor forhåndskontroll fra Datatilsynet. Ny personopplysningslov og personvernforordningen gjelder ikke når annet er bestemt i eller med hjemmel i lov. Dagens særlovgivning innen helse videreføres med lovtekniske endringer.

Implementering av ny personvernlovgivning i Sykehuset i Vestfold:

Administrerende direktør er ansvarlig for sykehusets behandling av personopplysninger. Noen av oppgavene er delegert internt til klinikksjefer og stabsdirektører som systemeiere for sine respektive systemer der personopplysninger behandles. De skal ha oversikt over alle systemene og ivareta internkontrollene innenfor sine enheter.

SiV har eget Personvernombud som ivaretar personverninteressene både til pasienter, publikum og ansatte i sykehuset. Personvernombudet gir råd og veiledning om behandling av personopplysninger slik at de behandles på en god måte og i tråd med regelverket.

Implementering av ny personvernlovgivning i SiV innebærer en bred tilnærming. Det har vært behov for å foreta kartlegging av dagens tilstand opp mot ny personvernlovgivning. Det gjennomføres bevisstgjøring og opplæring av ansatte. Det er nødvendig med et omfattende arbeid for å klargjøre prosedyrer og prosesser og tilpasninger i IKT-systemer samt involvering av ledere ved implementering og etterlevelse. Under følger en skjematisk fremstilling av arbeidet som pågått i Sykehuset i Vestfold:



Forankring:
Personvernombudet i SiV orienterte administrerende direktør og ledergruppen om ny personvernlovgivning i ledermøtet 14. mars 2018. Det ble besluttet oppstart av fase I - kartlegging.

Kartlegging:
Sykehuset skal ha oversikt over hvilke personopplysninger som behandles her og hva som er det rettslige grunnlaget for behandlingen. Det er et krav som gjelder også etter dagens lov. Sykehuset har oversikt over behandlingene. I løpet av mai/juni gjøres en kartlegging for å sikre en mer detaljert registrering av behandlinger i et felles kartleggingsverktøy (protokoll).

Kartleggingen gjøres i samarbeid med Sykehuspartner som er databehandler for en rekke av våre systemer. Kartlegging av andre systemer og med andre databehandlere, gjøres av IKT-seksjonen i SiV i samarbeid med klinikkene og stab/støtte-enhetene.

HR-direktøren gjennomfører på medarbeiderområdet kartlegging av hvilke system(er) som er involvert, hvilke personopplysninger som behandles, hvordan personopplysningene innhentes, om alle personopplysninger som innhentes er nødvendige, hvilke risikofaktorer som knytter seg til forhold til oppbevaring, hvordan redusere disse, sletting m.m. Kartleggingen gjøres prosessmessig; rekruttering, oppstart nyansatt, disiplinærsaker, lønnsoppgjør, bemannings- og driftsanalyser og utarbeidelse av bemanningsplaner.

<u>Gjennomføring og etterlevelse:</u>

Sykehuset etterlever langt på vei dagens krav til behandling av personopplysninger. Det utarbeides nå en handlingsplan for sikring av gjennomføring og etterlevelse. Den vil blant annet omfatte gjennomgang av sykehusets gjeldende rutiner for behandling av

personopplysninger. De vil bli oppdatert i henhold til nytt regelverk. Nye rutiner etableres der det er nødvendig.

Sykehuset har allerede et stort antall dokumenter i kvalitetssystemet som omhandler behandling av personopplysninger:

- Behandling av pasientopplysninger; Dokumenter om registrering, lagring, taushetsplikt, innsyn/utlevering, retting, sletting m. m. revideres. Det utarbeides nye retningslinjer for blant annet informasjon til pasienter og pårørende.
- Behandling av ansattopplysninger; Etter gjennomført kartlegging starter jobben med å sikre korrekt bruk og oppbevaring av personopplysninger. Endring av prosedyrer/ rutiner og arbeidsmetoder står sentralt. Det bør vurderes opplæringstiltak der nye systemer eller andre måter å jobbe på må implementeres.
- Kvalitets, innovasjons- og forskningsprosjekter; Det er behov for å endre styrende dokumenter vedrørende informasjon som gis til deltakere i prosjekter, måten vi godkjenner prosjekter på og hvordan vi lagrer data.
- Informasjonssikkerhet: Det er utarbeidet et omfattende, felles styringssystem for informasjonssikkerhet i Helse Sør-Øst. Hvert foretak har implementert det i kvalitetshåndboken sin. Dokumentene revideres nå av Regionalt Sikkerhets Råd opp mot ny personvernlovgivning.

Handlingsplanen vil også omfatte plan for opplæring og bevisstgjøring i sykehuset. Personvernombudet i SiV har gitt/gir opplæring av ledere og ansatte på ledermøter og fagdager. I tillegg har flere ledere og ansatte gjennomført eksterne kurs om ny lovgivning. Personvernombudene og fagmiljøene innen informasjonssikkerhet og juss i Helse sør-øst, samarbeider om implementeringen der det er hensiktsmessig.

Personvernombudet utarbeider nå en «Personvernerklæring» som omtaler sykehusets behandling av personopplysninger. Erklæringen legges på siv.no sammen med revidert, generell informasjon om personvern i SiV.

Adm. direktørs vurderinger:
Det er positivt at personvern blir regulert i tråd med teknologisk utvikling og internasjonalisering slik at både personvern og forutsigbarhet for databehandlerne blir ivaretatt

Arbeidet med implementering av ny personvernlovgivning i SiV er i gang. Så fremt Stortinget ikke vedtar vesentlige endringer i fremlagte forslag til ny personopplysningslov, vil kartleggingsfasen være avsluttet innen loven settes i kraft. Målet er at også gjennomføringsfasen skal være avsluttet da.

Administrerende direktør vil ha spesiell oppmerksomhet rettet mot oppfølging og praktisk implementering av endringer i fht. eksisterende lovgivning.

Vedlegg 1

Definisjoner

Personvern handler om retten til et privatliv og retten til å bestemme over egne personopplysninger. Personvernlovgivningen regulerer blant annet behandling av personopplysninger.

Personopplysning er en opplysning eller vurdering som kan knyttes til deg som enkeltperson, slik som for eksempel navn, adresse, telefonnummer, e-postadresse, IP-adresse, bilnummer, bilder, fingeravtrykk, irismønster, hodeform (for ansiktsgjenkjenning) og fødselsnummer (fødselsdato + personnummer).

Opplysninger om atferdsmønstre er også regnet som personopplysninger f eks. hvor du beveger deg i løpet av en dag og hva du søker etter på nettet.

Sensitive personopplysninger er opplysninger om rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning, at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling, ***helseforhold***, seksuelle forhold eller medlemskap i fagforeninger.

Behandling av personopplysninger: enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter

Behandlingsansvarlig: den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes (den dagelig ledelse=Adm. Dir)

Databehandler: den som behandler personopplysninger på vegne av den behandlingsansvarlige (eks. Sykehuspartner)

Den registrerte: Den opplysningene gjelder. I SiV er det både pasienter, ansatte og publikum.

Vedlegg 2 Datatilsynets punktliste

Nye personvernregler fra 2018. Hva betyr det for din virksomhet?

Hva blir nytt?

1

Alle norske virksomheter får nye plikter
Alle virksomheter må sette seg inn i den nye lovgivningen og finne ut hvilke nye plikter som gjelder dem. Ledelsen må sørge for å få på plass rutiner for å overholde de nye pliktene. Alle ansatte må følge de nye rutinene når reglene trer i kraft.

2

Alle skal ha en forståelig personvern-erklæring
Informasjon om hvordan din virksomhet behandler personopplysninger skal være lett tilgjengelig og skrevet på en forståelig måte. Det nye lovverket stiller strengere krav til informasjonens form og innhold enn dagens lovgivning. All informasjon som gis til barn, skal tilpasses barnas forståelsesnivå.

3

Alle skal vurdere risiko og personvernkonsekvenser
Dersom et tiltak utgjør en stor risiko for personvernet, må virksomheten også utrede hvilke personvernkonsekvenser det kan ha. Hvis utredningen viser at risikoen er stor og dere selv ikke kan redusere den, skal Datatilsynet involveres i forhåndsdrøftelser.

4

Alle skal bygge personvern inn i nye løsninger
De nye reglene stiller krav til at nye tiltak og systemer skal utarbeides på en mest mulig personvernvennlig måte. Dette kalles innebygd personvern. Den mest personvernvennlige innstillingen skal være standard i alle systemer.

5

Mange virksomheter må opprette personvernombud
Alle offentlige og mange private virksomheter skal opprette personvernombud. Et personvernombud er virksomhetens personvernekspert, og et bindeledd mellom ledelsen, de registrerte og Datatilsynet. Ombudet kan være en ansatt eller en profesjonell tredjepart.

6

Reglene gjelder også virksomheter utenfor Europa
Virksomheter som holder til utenfor Europa må også følge forordningen, dersom de tilbyr varer eller tjenester til borgere i et EU- eller EØS-land. Dette gjelder også om de ikke direkte tilbyr tjenester, men kartlegger adferden til europeiske borgere på nett. De som er etablert i flere land i Europa, skal bare trenge å snakke med personvernmyndighetene i det landet der de har sitt europeiske hovedkvarter.

7

Alle databehandlere får nye plikter
Databehandlere er virksomheter som behandler personopplysninger på oppdrag fra den ansvarlige virksomheten. Ofte er det snakk om leverandører av IT-tjenester. De nye reglene pålegger databehandlere å ha rutiner for innsamling og bruk av personopplysninger. Databehandlere skal også si ifra til oppdragsgiveren sin hvis de får instrukser som er i strid med loven. Oppdragsgiver skal også godkjenne databehandlerens underleverandører. Databehandlere kan også bli holdt økonomisk ansvarlig sammen med oppdragsgiver.

8

Alle bør samarbeide i egne nettverk og følge bransjenormer
De nye reglene oppmuntrer til sektorvis utforming av retningslinjer og bransjenormer. Om dere følger bransjenormer, vil dere ha de viktigste rutinene på plass. Datatilsynet skal godkjenne bransjenormene.

9

Alle får nye krav til avvikshåndtering
Reglene for håndtering av sikkerhetsbrudd blir strengere. Forordningen stiller krav til når det skal varsles, hva varselet skal inneholde og hvem som skal varsles. Kort sagt skal man si fra raskere og oftere enn man gjør i dag.

10

Alle må kunne oppfylle borgernes nye rettigheter
Den enkeltes rett til å kreve at hans eller hennes personopplysninger slettes blir styrket. Dette kalles «retten til å bli glemt». Norske og europeiske borgere vil blant annet kunne kreve å ta med seg personopplysningene sine fra en leverandør til en annen i et vanlig brukt filformat. Dette kalles «dataportabilitet». De kan også motsette seg profilering. Alle henvendelser fra borgere skal besvares innen en måned.

Hva bør dere gjøre nå?

1

Ha oversikt over hvilke personopplysninger dere behandler
Alle virksomheter som samler inn eller bruker personopplysninger skal ha oversikt over hvilke personopplysninger det er snakk om, hvor de kommer fra og hva som er det rettslige grunnlaget for behandlingen. Sørg for å ha en slik oversikt. Det er et krav som gjelder også etter dagens lov.

2

Sørg for å oppfylle dagens lovkrav
Overgangen til de nye reglene blir lettere om dere etterlever kravene i personopplysningsloven, som gjelder i Norge i dag. Har dere gode rutiner for internkontroll som fungerer etter hensikten og er kjent i organisasjonen, er det lettere å få oversikt over hva dere må endre.

3

Sett dere inn i det nye regelverket
Dere finner forordningsteksten på Datatilsynets nettsider. Der fyller vi også på med artikler om de nye reglene etter hvert som vi utarbeider dem.

4

Lag rutiner for å følge de nye reglene
Gå gjennom rutinene dere har for behandling av personopplysninger. Oppdater dem etter nytt regelverk der det trengs. Dokumenter de nye rutinene, og legg en plan for nødvendige endringer. Er systemene deres laget for å ivareta kravet til innebygd personvern, dataportabilitet og personvern som standardinnstilling? Klarer dere å fange opp og besvare henvendelser fra borgerne innen én måned? Endringer i systemer og rutiner tar tid. Begynn allerede nå!

datatilsynet.no/forordning