SUNNAAS SYKEHUS

Til styret i Sunnaas sykehus HF

21. september 2018

Sak 5318 Innføring av General Data Protection Regulation (GDPR)

Forslag til vedtak

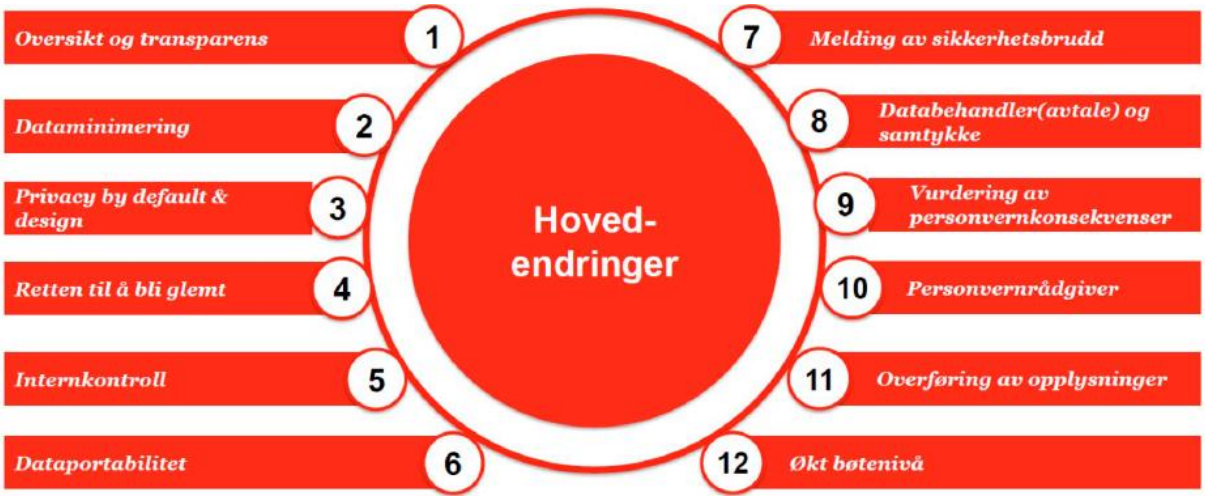
1. Styret vedtar General Data Protection Regulation (GDPR) som ble innført 20. juli 2018.
2. Styret ber administrerende direktør sikre implementering av forordningen for Sunnaas sykehus HF slik det fremgår av fremlagt statusrapport.

Bakgrunn for saken

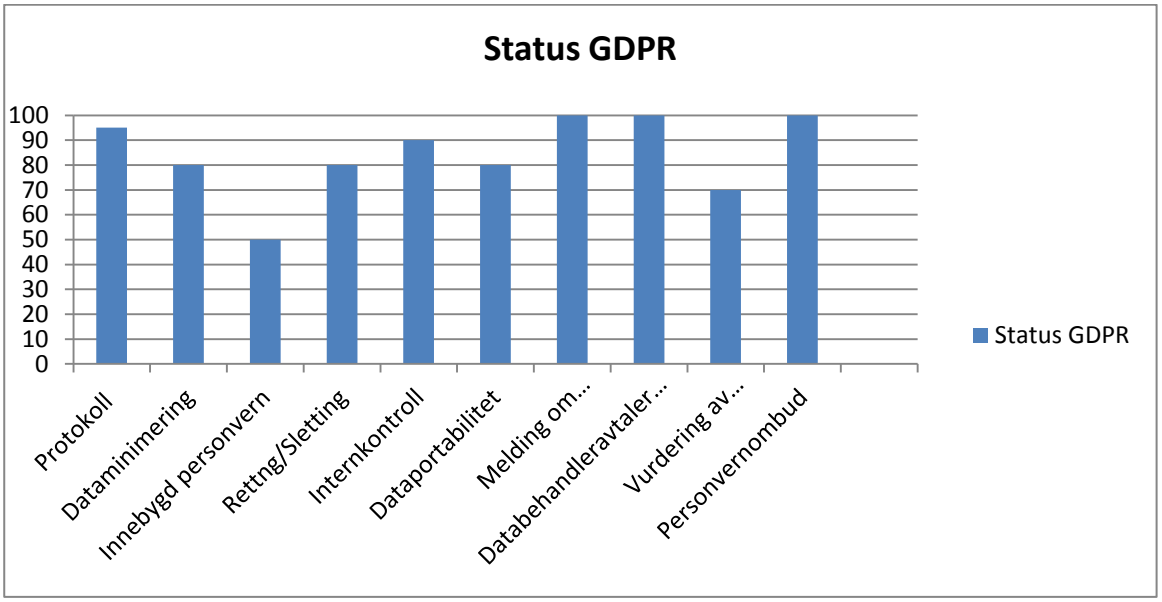
Innføring av den nye personvernloven 20. juli 2018, samt orienteringssak til styret 20.03.2018. Datatilsynets vedtak om pålegg, datert 28.06.2017.

Sammendrag og konklusjoner

Hovedendringer



Post- og besøksadresse: Sunnaas sykehus HF Bjørnemyrveien 11 1453 Bjørnemyr	Telefon: 66 96 90 00 Telefaks: 66 91 25 76	E-post: firmapost@sunnaas.no Bankkonto: 8601.72.22025 Foretaksnr.: 883 971 752 www.sunnaas.no



1 Oversikt og transparens – art. 30 i forordningen som omhandler protokoll

Denne protokollen er grunnlaget for å ha kontroll over våre databehandlinger på Sunnaas sykehus HF. Dette har også vært en av de mest krevende oppgavene, da det har involvert ressurser fra klinikk, ekstern konsulent og administrasjon. Det må sikres en kontinuerlig oppdatert oversikt, og følgelig må det integreres i internkontrollen. Systemeiere må bevisstgjøres, og en fortløpende oppdatering av protokollen må gjøres. Rutine må utarbeides og legges i Heliks. Dette kravet er ikke nytt, men ble skjerpet ved innføringen av GDPR.

Status: 90 %

2 De registrertes rettigheter (Blant annet nr. 2, 4, 6)

1. Dataminimering
2. Retting/Sletting
3. Informasjon
4. Dataportabilitet

Viktige rettigheter som forsterkes ved innføringen av GDPR. Flere av rettighetene har eksistert også før det nye regelverket, men blitt styrket i den nye forordningen. Hovedtyngden av endringene i regelverket går på at de registrerte skal få tydelig informasjon om hvordan vi behandler data og hva formålet med behandlingen er. I hovedsak er Sunnaas sin behandling nødvendig for å yte helsehjelp.

I arbeidet med å tydeliggjøre informasjon ut til de registrerte er det gjennomført regionale prosesser som går på oppdatering og konkretisering av behandlingen av informasjon på våre nettsider. De er også oppdatert med informasjon om kontaktinformasjon til personvernombudet som det stilles krav til. Andre prosesser her går på informasjon til ansatte, herunder personvernerklæring og samtykker ved innsamling av data i ansettelsesprosessen i den grad

tredjeparter benyttes. Brev som sendes ut fra foretaket (via DIPS) og TRS kompetansesenter for sjeldne diagnoser til de registrerte skal oppdateres med nødvendig informasjon, og dette jobbes det også med regionalt der det berører DIPS. For TRS er informasjon og brevmaler oppdatert med nødvendig informasjon.

Videre er det krav til gjennomsiktighet, tidsfrister for sammenstilling av informasjon mm. Dette går på interne rutiner som enten må oppdateres eller utarbeides. Sammen med dette må det informeres ut til ansatte slik at de som er involvert i de ulike prosessene er oppdatert i endringene.

Det som gjenstår er å fullføre prosessene som er påbegynt, og det innebærer i hovedsak detaljeringsnivå av tekst i ulike dokumenter. Vi vil på bakgrunn av dette mene at vi er nesten i mål hva angår informasjon og tydeliggjøring, men at enkelte dokumenter må oppdateres og implementeres i Heliks.

Status: 80 %

3 Internkontroll

Revisjon av styringssystem for informasjonssikkerhet (regional prosess) tar noe lengre tid enn planlagt. Omtrent 80 % er gjennomført, men ingenting er implementert enda. Revisjonen gjøres i fellesskap blant helseforetakene, og når dette er fullført, må det opp i FTL for beslutning før det implementeres Sunnaas sykehus.

Mønstergjenkjenning forventes å komme i løpet av høsten 2018, noe som vil styrke loggkontrollen. Dette vil kreve ressurser i helseforetaket, både på HR-siden og for loggkontrollør. Foreløpige tall indikerer økt avvik knyttet til uautoriserte oppslag i journal.

Internkontrollen bør styrkes gjennom dokumentasjon, og er hensiktsmessig for å vise til etterlevelse. Systemer som omfatter internkontroll må styrkes, men det følger mindre krav til detaljer ved innføringen av det nye regelverket. Derimot vektlegges bransjenormer sterkere, der Normen er gjeldende for helsesektoren. Denne er til høring hos Datatilsynet nå, og dersom den blir godkjent vil en dokumentert etterlevelse av denne være fordelaktig. På bakgrunn av dette er det hensiktsmessig å utforme en dokumenterbar og systematisk internkontroll som beror på Normen.

Vedrørende internkontroll er det en kontinuerlig prosess, og det er ikke en ny plikt for virksomheter. Derimot er det fordelaktig at det jobbes systematisk med dette for å styrke oss på informasjonssikkerhet og personvern fremover.

Status: 90 %

4 Melding om sikkerhetsbrudd

Rutine utarbeidet, og klar for innføring i Heliks.

Status: 100 %

5 Databehandleravtale og samtykke

Databehandleravtale mellom Sykehuspartner og Sunnaas sykehus er oppdatert og signert av begge parter. Utarbeidelse av mal til databehandleravtale mellom Sunnaas sykehus og underleverandører er også ferdig, men er ute på høring/gjennomgang hos jurist ved RHF-et.

Samtykker er sendt ut etter innføring av GDPR, der de fleste har vært innom personvernombud for gjennomlesing før godkjenning. Det anses hensiktsmessig å utarbeide maler for ulike samtykkeskjema, men ikke en nødvendighet for å oppfylle regelverket. Utarbeidelse av mal er ønskelig for å gjøre det lettere for den enkelte som trenger å ta dette i bruk.

Status: 100 %

6 Innebygd personvern

Dette er en ny plikt som følger av personvernloven. Det innebærer at man skal tenke personvern i alle faser, både ved arbeidsprosesser og teknologi. Informasjon og bevisstgjøring når det kommer til innebygd personvern er noe som må utarbeides og gjennomføres. Systemeiere må bevisstgjøres sitt ansvar når det gjelder sine systemer, og det må utarbeides informasjon om denne plikten. Innovasjon og teknologi er særdeles relevant her, da man tidlig i fasene må tenke innebygd personvern.

Hva gjelder tekniske systemer må man tenke personvern som standardinnstilling, og sikre at man bygger opp systemene på personvernprinsippene. Det må gjennomgås rutiner som sikrer dataminimering. Således henger innebygd personvern tett sammen med de registrertes rettigheter.

Status: 50 %

7 Vurdering av personvernkonsekvenser (DPIA)

Dette er en ny plikt som følger av regelverket, og det er mye diskutert regionalt. Det er ikke utarbeidet konkrete retningslinjer vedrørende dette, men det finnes malverk som kan tas i bruk fra Direktoratet for e-helse. På den måten kan vi sikre at nødvendig prosess dokumenteres dersom det er behov for dette. Tidspunktet for når man skal gjennomføre personvernkonsekvenser er ikke tydelig definert, og dermed er det også gjenstand for diskusjoner og dialog omkring dette. For Sunnaas sykehus må det utarbeides en skriftlig rutine som sier noe om når, hvor og hvem som skal involveres i dette arbeidet.

Status: 70 %

8 Personvernombud

Definert rollen personvernombud, med beskrivelse av tilhørende ansvar og oppgaver. Klar til å legges inn i Heliks.

Status: 100 %

9 Andre betraktninger

Når det gjelder etterlevelse av regelverk er det alltid rom for forbedring og styrking. Dette gjelder både lokalt og regionalt, og det vil være stor aktivitet på dette området framover. Nedenfor er det kort innledning til to regionale aktiviteter som snart settes i gang.

- Helse Sør-Øst RHF vil ta kontakt med helseforetakene for en oppfølging i regionen for å bidra i arbeidet med GDPR. Disse var invitert med på siste regionale sikkerhetsfaglige råd for å få innspill og bli kjent med arbeidet som er gjort hittil.
- Det er også vedtatt en arbeidsgruppe der fire ulike helseforetak (Sunnaas sykehus, sykehuset Østfold, Oslo universitetssykehus, og Sørlandet sykehus) skal jobbe sammen med Sykehuspartner der ett av de fire hovedprosjektene er GDPR. Formålet er å identifisere og følge opp nødvendige tiltak og tilpasninger med hensyn til nytt regelverk.

10 Oppsummering

Tross at den skriftlige dokumentasjonen snart nærmer seg slutten innebærer etterlevelse av regelverket også kontinuerlig arbeid med styrking av arbeidsprosesser og tilpasninger til nytt regelverk. Økt krav til dokumentasjon og etterlevelse av bransjenormer og internkontroll er en fortløpende prosess som er nødvendig for å etterleve regelverket. Samtidig er bevisstgjøring og holdningsendring for å styrke sikkerhetskulturen en gradvis prosess.

Som kjent har vi jobbet mye med vedtaket fra Datatilsynet den siste tiden, som omhandler blant annet manglende selvstendige vurderinger og dokumentasjon av tilgangsstyring. Vedtaket illustrerer i så måte utilstrekkelig etterlevelse av det gamle regelverket, og gjenspeiler således også et ressursbehov. Det presiseres at etterlevelse av regelverket beror på det kontinuerlige arbeidet som skal gjøres fremover, både ved å avdekke tilpasninger som følge av regelverket, men også prosesser for å ivareta de nye kravene. Som nevnt er det flere nye prosesser og teknologi som kommer som vil øke kravene til innsats, herunder mønstergjenkjenning, internkontroll, DPIA og innebygd personvern.

På bakgrunn av overnevnte status over prosessene er vi godt i gang med å etablere nye rutiner som sikrer at vi har forutsetninger for å etterleve den nye personvernloven. De fleste av kravene gjaldt også tidligere, men har gjerne blitt styrket i overgangen. Selv om flere av rutinene og styringssystemet for informasjonssikkerhet ikke er oppdatert i kvalitetssystemet enda, er vi slik vi ser det i stor grad GDPR-compliant.

Einar Magnus Strand
Administrerende direktør