SUNNAAS SYKEHUS

Til styret i Sunnaas sykehus HF

18. desember 2018

Sak 85/18 Innføring General Data Protection Regulation (GDPR) - status

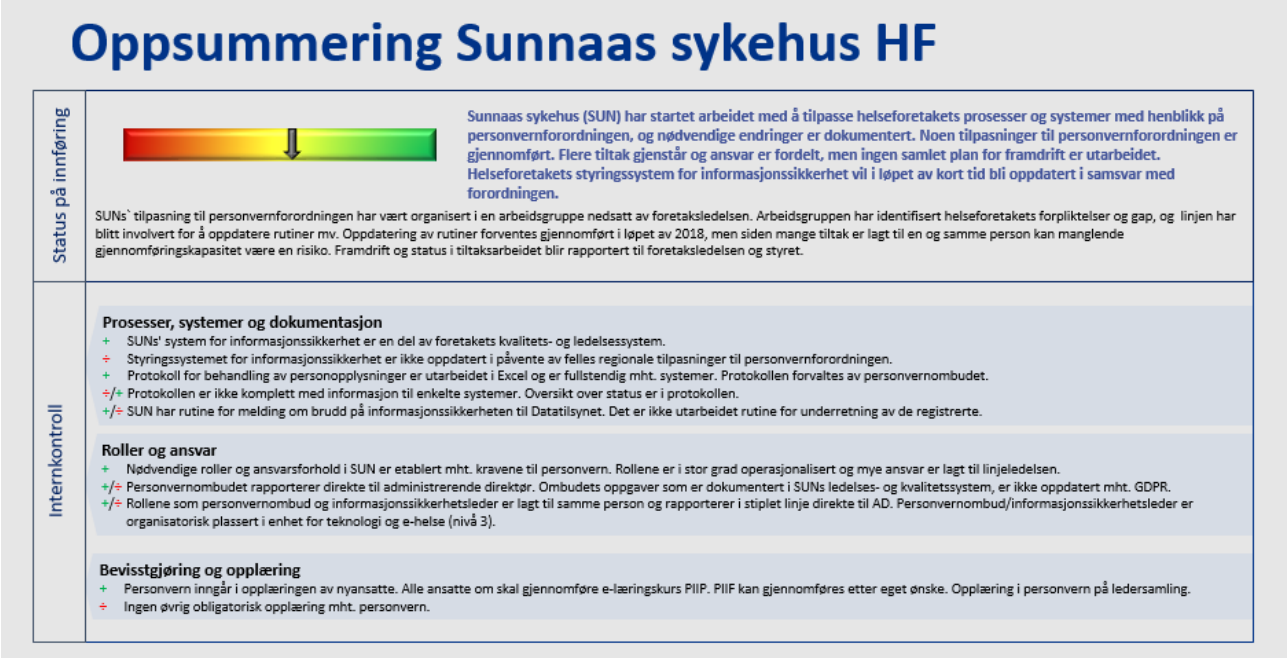
Innføring av den nye personvernloven (GDPR) ble vedtatt 20. juli 2018. Det har i forkant av dette vedtaket vært prosess med forberedelser siden høsten 2017. Styret ved Sunnaas sykehus HF ble orientert om status i forberedelsesarbeidet i styremøte 20. mars 2018. Etter vedtak om innføring av den nye forordningen ble det lagt frem en statusorientering til styret 20. september 2018.

Forslag til vedtak
Styret tar saken til orientering.

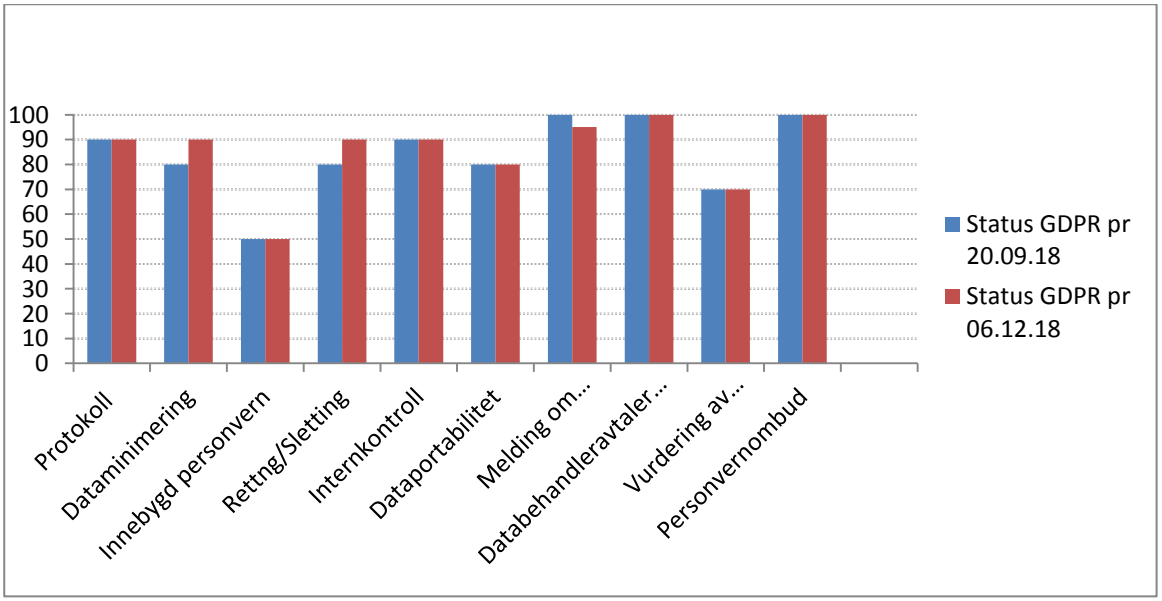
Sammendrag og konklusjoner
Krav om personvernombud for forskning ved eget foretak er et nytt krav som kom med det nye regelverket. Tidligere var Oslo Universitetssykehus HF (OUS) personvernombud for forskning for oss på Sunnaas, men dette er ikke lenger mulig da det kreves at hver virksomhet (juridisk enhet) har eget ombud. På grunn av interne kapasitets- og kompetanseutfordringer er det valgt å inngå avtale med NSD (Norske senter for forskningsdata) som vil gjøre personverntjenester knyttet til forskning. Dette fritar ikke Sunnaas fra vårt ansvar, men det vil hjelpe ved behandling av saker i forbindelse med forskning. Her må det etableres en prosess som sikrer at personvernombudet er involvert i sakene, og kjenner til de ulike forsknings- og kvalitetsprosjektene selv om NSD står for saksbehandlingen. Videre må Sunnaas definere og utarbeide en prosess for personvernkonsekvensvurderinger (DPIA) for forskning i de tilfellene dette er nødvendig.

Konsernrevisjonen var på rådgivende oppdrag hos Sunnaas 30.10.2018, og har på bakgrunn av dette kommet med en midlertidig rapport på vårt arbeid i forbindelse med GDPR. Gjennomgangen avdekket blant annet sårbarhet ved at mye av arbeidet relatert til personvernforordningen er lagt til én person. Foretaket er i stor grad avhengig av personvernombudets kompetanse og arbeid for å få plass nødvendige retningslinjer og prosesser. Oppsummeringen fra konsernrevisjonen kan ses nedenfor. Mer utfyllende rapport er planlagt å komme i løpet av desember 2018 når de har gjennomført oppdraget ved alle helseforetakene i Helse Sør-Øst.

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



Konsernrevisjonens rapport samstemmer godt med våre evalueringer av arbeidet og status. Nedenfor er oversikten over status levert til styret 20. september og 18.12.2018.



For å gjennomføre implementeringen av personvernforordningen innen rimelig tid er det laget en implementeringsplan for personvernforordningen som består av flere oppgaver (43 oppgaver pr. 05.12). Denne ligger vedlagt. Fordi dette er et regelverk som griper inn i samtlige deler av foretaket er oppgavene fordelt ut til flere personer og avdelinger ved foretaket. Det er satt en frist for å ha gjennomført samtlige oppgaver innen 01.05.2019.

Hensikten med å fordele oppgavene er todelt;

1. Vi får raskere progresjon på implementering av regelverket
2. Ansvarliggjøre sentrale personer og avdelinger i foretaket, samt skape god sikkerhetskultur

For å kunne bygge en god sikkerhetskultur er det nødvendig å bevisstgjøre, informere og dele kunnskap for å skape en positiv endring. Ved å involvere flere personer vil dette forhåpentligvis skape gode synergieffekter, der flere får eierskap til etterlevelse av regelverket – samt at man får spredd kunnskap om regelverket til flere. For å kunne etterleve i tilstrekkelig grad er det helt nødvendig at samtlige ansatte kjenner til det.

Nedenfor følger en kort oppdatering innenfor de ulike områdene som har vært hovedområdene under orientering om GDPR og status underveis. Det er satt ny status under de ulike områdene, som baserer seg på en kvalitativ vurdering fra personvernombudet.

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

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. Det er planlagt innleie av konsulent for å bistå arbeidet med å ferdigstille protokollen og arbeidet knyttet til bevisstgjøring av systemeiere og systemansvarlige, og utarbeide plan for oppdatering av protokoll samt innebygd personvern. Status er at vi ikke har fått tak i eksterne ressurser her, så foreløpig er dette en oppgave som tilfaller informasjonssikkerhetsleder/personvernombud. Protokollen er i stor grad ferdigstilt, men det siste er tidkrevende prosesser.

Status pr 20.09.18: 90 % **Status pr 06.12.18:** 90 %

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

Det som gjenstår er å fullføre prosessene som er påbegynt, og det innebærer i hovedsak detaljeringsnivå av tekst i ulike dokumenter. Vi er nesten i mål med dette, og det som gjenstår skal gjøres av kvalitetsrådgivere i samarbeid med logoped.

Status pr 20.09.18: 80 % **Status pr 06.12.18:** 90 %

3 Internkontroll

Revisjon av styringssystem for informasjonssikkerhet (regional prosess) er gjennomført regionalt, og skal nå implementeres i Heliks. Frist for gjennomføring er 31.12.2018.

Det er etablert gode rutiner for manuell loggkontroll frem til logganalyse kommer på plass, forhåpentligvis i 2019.

Status pr 20.09.18: 90 % **Status pr 06.12.18:** 90 %

4 Melding om sikkerhetsbrudd

Rutine utarbeidet, og klar for innføring i Heliks. Tilbakefall på dette fordi vi må også innføre en rutine som innebærer melding til de berørte dersom det er behov. Dette kommer av på grad av risiko i de tilfellene det oppstår et sikkerhetsbrudd.

Status pr 20.09.18: 100 % **Status pr 06.12.18:** 95 %

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 ferdig og i bruk.

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 pr 20.09.18: 100 % **Status pr 06.12.18:** 100 %

6 Innebygd personvern

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.

Lite progresjon rundt dette kravet. Gjennomgang av samtlige systemer og plan for dette må utarbeides. Arbeid med oversikt over systemer, systemeiere og systemansvarlig er påbegynt.

Status pr 20.09.18: 50 % **Status pr 06.12.18:** 50 %

7 Vurdering av personvernkonsekvenser

Det er ikke utarbeidet konkrete retningslinjer vedrørende dette, men det finnes malverk som kan tas i bruk fra Direktoratet for e-helse. Således sikres nødvendig prosess dersom behov. Sunnaas sykehus må utarbeide skriftlig rutine som sier noe om når, hvor og hvem som skal involveres i dette arbeidet.

Status pr 20.09.18: 70 % **Status pr 06.12.18:** 70 %

8 Personvernombud

Definert rollen personvernombud, med beskrivelse av tilhørende ansvar og oppgaver. Klar til å legges inn i Heliks. (Dokumentstyringssystem for Sunnaas)

Status pr 20.09.18: 100 % **Status pr 06.12.18:** 100 %

9 Andre betraktninger

Det er påbegynt en vurdering av organiseringen av personvernombudet og informasjonssikkerhetsleder der ledelsen er involvert. Dette er spesielt med tanke på å oppfylle kravet om uavhengighet for personvernombudet, og avvik fra regionalt styringssystem for informasjonssikkerhet hva angår organisering av informasjonssikkerhetsleder. Virksomheten skal stille til rådighet de ressurser som er nødvendige for at personvernombudet skal kunne utføre sine oppgaver (https://www.datatilsynet.no/rettigheter-og-plikter, samt artikkel 38 og 39 i forordningen). En gjennomgang av eksisterende organisering og ressurssituasjon bør dokumentere hvilke vurderinger og valg som er gjort med hensyn til sikkerhetsarbeidet på Sunnaas, med fokus på innføringen av personvernregelverket. Spesielt bør det dokumenteres hva som er vektlagt ved beslutninger om ressurser og kompetanse for å kunne utføre oppgaven som personvernombud på en tilstrekkelig måte. En framtidig organisering og bemanning må også ha som siktemål å redusere sårbarheten ved at oppgaver og ansvar fordeles på flere funksjoner (ref. konsernrevisjonens kommentarer).

Styret er gjennom driftsorientering fra administrerende direktør i styremøte desember 2017 gjort kjent med etablering av sikkerhetsorganisasjon i sykehuset og implementering av denne gjennom utarbeiding og godkjenning av ulike dokumenter og funksjoner det er krav om. Administrasjonen gjorde i etterkant beslutning om å etablere et felles utvalg for beredskap og sikkerhet i sykehuset der medlemmer av utvalget utgjør sykehusets beredskapsledelse. Utvalget/beredskapsledelsen er godt representativ med medlemmer fra Foretaksledelsen. Det er oppnevnt flere underutvalg, herunder underutvalg for planlegging og gjennomføring av beredskapsøvelser og opplæring samt underutvalg for sikkerhetsorganisasjon og oppfølging av arbeidet med forebyggende

sikkerhetsarbeid og gradert dokumentasjon/informasjon. Alle medlemmer av sikkerhetsorganisasjonen er sikkerhetsklarert.

Det er gjennom 2018 gjennomført en intern prosess for synliggjøring av alle oppgaver og ressurs- og kompetansebehov for å kunne ivareta krav og sikre forsvarlig drift for områdene sikkerhet, beredskap og informasjonssikkerhet/personvern. Det er samtidig gjennomført en evaluering for hvordan nytt beredskaps og sikkerhetsutvalg/beredskapsledelse med underutvalg fungerer og med innspill til forbedringer. Administrasjonen har sett behov for å styrke fagområdet informasjonssikkerhet og personvern med økte ressurser tilsvarende 50 % stilling fra januar 2019. Videre er det besluttet å gjennomføre et prosessarbeid gjennom 1.halvår 2019 med mål å legge frem forslag til endelig organisering av området beredskap, sikkerhet og informasjonssikkerhet – personvern samt behov for ressurser og kompetanse for det totale tjenesteområdet.

10 Oppsummering

Oppsummert er status på implementeringen av GDPR i stor grad lik som den var i september 2018. Det settes en frist til 01.05.2019 for å komme i mål med de ulike oppgavene, men dette beror på at de som tildeles oppgaver får frigitt tid fra eventuelle andre oppgaver for å gjennomføre det. Oppgavene deles ut bredere enn det som var tiltenkt med mandat for arbeidsgruppen, og dette skyldes delvis ressursbehovet på fagfeltet informasjonssikkerhet og personvern som redegjort for i forrige status av 20. september d.å., men også fordi flere personer fra arbeidsgruppen har sluttet eller er i permisjon.

Det er satt av midler til et halvt årsverk ekstra fra 2019 som skal styrke både arbeidet med generell sikkerhetsledelse og personvern i foretaket. Inntil ansettelse har skjedd ønskes midlene disponert til styrking av arbeidet rundt implementeringen GDPR ved hjelp av innleide ressurser.

Bakgrunn for saken
Innføring av den nye personvernloven 20. juli 2018
Orienteringssak til styret 20.03.2018.
Status GDPR 20.09.2018

Einar Magnus Strand
Administrerende direktør

Vedlegg
Innføring General Data Protection Regulation - Fremdriftsplan