HELSE SØR-ØST

Organisering av personvern- og informasjonssikkerhetsarbeidet

Versjon	**Dato**	**Behandling/endring**	**Godkjent av**
1.0	22.12.2016		
1.1	23.10.2018		
2.0	9.12.2021	Større omarbeiding. *NO-21 – Internkontroll informasjonssikkerhet* er tatt inn. Personvern er beskrevet mer systematisk. Tilsluttet i direktørmøtet 2. desember 2021 med de innspill som kom i møtet.	Øyvind Grinde
2.1	24.6.2025	Oppdatering i henhold til styresak om styrket arbeid med personvern, inkludert omtale av nye roller. Tilsluttet i direktørmøtet 12. juni 2025 med de innspill som kom i møtet, samt frist til 20. juni for eventuelt ytterligere innspill.	Øyvind Grinde

1 Hensikt og omfang

Formålet med dette dokument er å klargjøre ansvar og oppgaver på informasjonssikkerhets- og personvernområdet, som del av helseforetakets styringssystem for informasjonssikkerhet.

1.1 Målgruppe

Dette dokumentet er relevant for alle ansatte. Dokumentet er spesielt relevant for ledere på alle nivåer, informasjonssikkerhetsleder, fagressurser innen personvern og konsernfelles personvern-ombud.

1.2 Struktur

Kapittel 2 beskriver hvilke oppgaver som skal utføres for å etterleve lover og regler og for å være henhold til den internasjonalt anerkjente standarden for ledelsessystem for informasjonssikkerhet (NS-EN ISO/IEC 27001) og standarden for tillegg for personvern (NS-EN ISO/IEC 27701). Kapitlet beskriver ikke hvem som har ansvar for arbeidsoppgavene og hvordan de utføres. Det gjøres i kapittel 3 og 4.

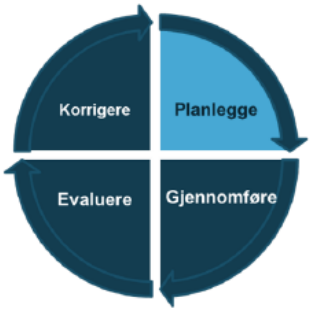
Kapittel 3 beskriver hvordan ansvarsområdene fordeles mellom helseforetakene i foretaksgruppen.

Kapittel 4 beskriver hvordan ansvar for arbeidsoppgavene fordeles internt i et helseforetak på de områder helseforetakene er enige om at det ikke bør være forskjeller mellom helseforetakene. Behov for å beskrive ansvar for arbeidsoppgaver utover dette er opp til hvert enkelt helseforetak.

2 Systematisk arbeid med informasjonssikkerhet og personvern

Personvern- og informasjonssikkerhetsarbeidet inngår som en del av den helhetlige virksomhets-styring i helseforetaket, jf. Rammeverk for virksomhetsstyring i Helse Sør-Øst.[1] God virksomhets-styring skal understøtte tydelige prioriteringer og bidra til at ledere på alle nivåer retter oppmerksomheten mot de deler av virksomheten som er vesentlig for måloppnåelse.

Arbeidet på personvern- og informasjonssikkerhetsområdet skal støtte opp under virksomhetsmålene til helseforetakene og baseres på samme forbedringshjul som for øvrig virksomhetsstyring. Arbeidet skal være innrettet på en effektiv måte innen fastsatte rammer (økonomiske o.a.) og slik at virksomhetsmålene nås, herunder at regelverk følges.



Figur 1 Forbedringshjul, fra Rammeverk for virksomhetsstyring i Helse Sør-Øst

Helse Sør-Øst har på personvern- og informasjonssikkerhets-området tatt utgangspunkt i Digitaliseringsdirektoratets veiledning til utformingen av internkontroll. Forklaringsmodellen under viser hovedaktivitetene i dette internkontrollarbeidet, samt hvordan målrettet kommunikasjon binder de øvrige aktivitetene sammen. Hver av hovedaktivitetene består av et sett delaktiviteter, som beskrives i delkapitlene nedenfor. De er kjernen i internkontrollarbeidet og skal gjennomføres systematisk.

[1] Rammeverket fikk tilslutning i Styremøte for Helse Sør-Øst RHF 24.9.2020, styresak 107/2020

Figur 2 Systematiske aktiviteter i internkontrollen, fra Digitaliseringsdirektoratets veiledning

Internkontrollen i Helse Sør-Øst skal være risikobasert. Policyer og prosedyrer innen informasjonssikkerhet og personvern skal etableres der risikoen tilsier det.

2.1 Ledelsens styring og oppfølging

2.1.1 Ledelsens gjennomgang

Ledelsen skal minimum årlig gå gjennom status for internkontroll på personvern- og informasjonssikkerhetsområdet. Formålet er å:

- avklare status på helseforetakets samlede internkontrollarbeid innen personvern og informasjonssikkerhet. Dette inkluderer minimum å ha oversikt over
  - sikkerhetstilstanden og de største informasjonssikkerhetsrisikoer i helseforetaket,
  - personverntilstanden og de største risikoer for manglende etterlevelse av personvernforpliktelser
- reagere og følge opp der det er nødvendig.

Ledelsen skal på bakgrunn av gjennomgangen gi eventuelle tilleggsføringer for helseforetakets internkontrollarbeid.

2.1.2 Øvrige aktiviteter

Ledere på alle nivå har også en viktig rolle i hovedaktiviteten *Ledelsens styring og oppfølging*. De er ansvarlig for systematisk gjennomføring av følgende aktiviteter:

- delegere og følge opp informasjonssikkerhets- og personvernarbeidet gjennom linjen
- sikre tilstrekkelig ressursmessig prioritering av området, innen gitte økonomiske rammer
- kommunisere viktigheten av egnet informasjonssikkerhet og godt personvern
- løfte og håndtere problemstillinger gjennom linjen
- beredskap og krisehåndtering

2.2 Risikovurderinger på informasjonssikkerhetsområdet

Internkontroll handler om risikostyring. Risikovurdering er den grunnleggende aktiviteten i risikostyringen.

Relevante risikoer skal identifiseres og deres størrelse skal anslås, slik at de kan prioriteres og håndteres på egnet måte.

Som informasjonssikkerhetsrisiko regnes risiko knyttet til brudd på informasjonens konfidensialitet, integritet eller tilgjengelighet.

2.3 Risikohåndtering på informasjonssikkerhetsområdet

På bakgrunn av risikovurderingen skal risikoreduserende tiltak vurderes, og risikoer håndteres i henhold til kriterier for aksept av risiko.

Følgende aktiviteter er en del av *Risikohåndteringen*:

- foreslå håndtering av risikoer
- godkjenne forslag til risikohåndtering
- iverksette godkjente tiltak, herunder
    - utforme og implementere sikkerhetstiltakene
    - oppdatere fellessikring og tilleggssikring

2.4 Overvåkning og hendelseshåndtering på informasjonssikkerhetsområdet

Uønskede hendelser, avvik og informasjonssikkerhetsbrudd skal oppdages og håndteres.

Overvåking er et sikkerhetstiltak som velges og utformes i risikohåndteringen på linje med øvrige tiltak. Slike tiltak skal inneholde informasjon om hva som skal overvåkes, hvem som er ansvarlig for overvåkingen og hvordan resultatet av overvåkingen skal rapporteres.

Hendelser, avvik og informasjonssikkerhetsbrudd skal rapporteres og følges opp i henhold til rutiner.

2.5 Risikobasert personvernarbeid (risikovurdering, -håndtering og overvåking på personvernområdet)

Helseforetakene skal innrette personvernarbeidet basert på risiko for de registrertes friheter og rettigheter. God informasjonssikkerhet er en vesentlig del av å sikre personvernet. Dette adresseres i kapittel 2.2, 2.3 og 2.4 ovenfor.[2]

Helseforetaket skal også ha tilstrekkelig oversikt over annen personvernrisiko[3]. Dette innebærer blant annet at det må vurdere risiko for manglende etterlevelse av personvernkrav, som krav til rettslig grunnlag for behandling, at opplysningene som behandles er adekvate og begrenset til det som er nødvendig for formålene (dataminimering), innsynsrettigheter og informasjonsplikter,

[2] Jf. personvernforordningen artikkel 32

[3] Jf. personvernforordningen artikkel 24

innebygd personvern, rett til dataportabilitet ved samtykke- og avtalebasert innsamling, bestemmelser om protokoll, databehandleravtaler og personvernkonsekvensvurdering.

Der risikoen eller forholdene for øvrig tilsier det, skal det iverksettes egnede tiltak for å møte risikoen.[4] Slike tiltak kan eksempelvis være at foretaksgruppen eller det enkelte helseforetaket utarbeider retningslinjer eller andre sannsynlighets- eller konsekvensreduserende tiltak.

Så langt det passer bør prosesser beskrevet for informasjonssikkerhetsområdet benyttes også på personvernområdet, for å få en helhetlig internkontroll.

2.6 Måling, evaluering og revisjon

Det skal systematisk vurderes om risikoreduserende tiltak fungerer, om regelverk etterleves og om internkontrollarbeidet rundt om i helseforetaket blir gjennomført som forutsatt.

I tillegg skal de som har ansvar for tiltak, vurdere om tiltakene fungerer som forutsatt.

2.7 Kompetanse- og kulturutvikling

Identifisering av behov for kompetanse- og kulturutvikling skal gjøres løpende som en del av internkontrollarbeidet i helseforetaket. Dette skal gjøres av ledere på alle nivå og for alle ansvarsområder. Når det er identifisert et behov skal det gjennomføres hensiktsmessige tiltak.

2.8 Kommunikasjon

Kommunikasjon binder sammen de andre hoved- og delaktivitetene samt aktørene som utfører disse.

Helseforetakets kommunikasjon med personer utenfor helseforetaket skal skje i samsvar med policy og retningslinjer for ekstern kommunikasjon. Lovpålagt taushetsplikt og offentlighetslovens bestemmelser om unntatt offentlighet og meroffentlighet skal ligge til grunn for all kommunikasjon.

3 Foretakenes ansvar for informasjonssikkerhet og personvern

Foretakene har ulikt ansvar for informasjonssikkerhet og personvern.

3.1 Helseforetak

Helseforetaket skal sørge for egnet informasjonssikkerhet og godt personvern, slik at helsetjenester tilbys med tilstrekkelig kvalitet og tilgjengelighet iht. krav i lov- og avtale. I dette ligger blant annet krav til internkontroll iht. kapittel 2 og relevant regelverk[5].

Helseforetaket er dataansvarlig iht. personvernforordningen.

[4] Jf. personvernforordningen artikkel 24 nr 2.

[5] Herunder forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten, FOR-2016-10-28-1250

Bruk av databehandler endrer ikke foretakets selvstendige ansvar for informasjonssikkerhet og personvern. Krav og forventninger til databehandlere, må kommuniseres klart og følges opp for å sikre at sikkerhetsmålsettingene til helseforetaket oppnås.

Helseforetaket skal:

- Sørge for at arbeidet med personvern og informasjonssikkerhet er risikobasert og at det er en integrert del av virksomhetens risikostyring. Helseforetaket skal ha tilstrekkelig oversikt over risikoer ved informasjonsbehandlingen, samt personvern- og sikkerhetstilstanden herunder:
    - Sørge for at risiko håndteres på egnet måte og at det fastsettes hvem som kan akseptere restrisiko på informasjonssikkerhetsområdet, i tråd med fastsatte regionale rammer, jf. NO-5[6].
    - Etablere sikkerhetstiltak i samsvar med prinsippet om at sikkerhetsmessig lønnsomme tiltak skal iverksettes, jf. NO-5.
    - Sørge for evaluering og kontinuerlig forbedring av arbeidet med personvern og informasjonssikkerhet.
- Sørge for at roller på personvern- og informasjonssikkerhetsområdet er tydelig identifisert og beskrevet, i samsvar med kapittel 4 og med ev. presiseringer og suppleringer. Helseforetaket skal sørge for at motstridende forpliktelser og ansvarsområder holdes adskilt der det er relevant innen personvern og informasjonssikkerhet.
- Følge regionale føringer for informasjonssikkerhet og personvern, gitt i foretaksmøtet, med mindre unntak er besluttet av helseforetakets styre. I dette ligger blant annet krav om at
    - helseforetaket skal ta hensyn til hvordan informasjonssikkerhetsrisiko vurderes i andre foretak (jf. mål og strategi)
    - dersom to helseforetak ikke blir enige om en informasjonssikkerhetsrisiko kan aksepteres, skal saken drøftes med Helse Sør-Øst RHF[7]
    - helseforetaket skal benytte Sykehuspartner HF som databehandler og følge Sykehuspartner HFs bruksvilkår for de tjenestene de tilbyr[8]
- Sette krav i avtaler til leverandørers informasjonssikkerhet og personvern. Databehandler-avtale skal være på plass før personopplysninger behandles av en databehandler.
- Rapportere i henhold til bestillinger og gi råd til Helse Sør-Øst RHF om eventuelle saker som krever oppmerksomhet og eventuelt avgjørelse.

3.2 Helse Sør-Øst RHF

Det regionale helseforetaket har et sørge-for-ansvar for spesialisthelsetjenesten i regionen, jf. spesialisthelsetjenesteloven § 2-1a.

Regionalt helseforetak skal sørge for at foretaksgruppen har et effektivt informasjonssikkerhets- og personvernarbeid som gir egnet informasjonssikkerhet og godt personvern. Regionalt helseforetak skal:

- Sørge for at det overordnet er en samlet og lik håndtering av informasjonssikkerhet og personvern i regionen, blant annet ved å:

[6] NO-5 - Kriterier for vurdering og aksept av risiko for informasjonssikkerhet

[7] Råd fra Datatilsynet, Helsetilsynet, o.a. kan være relevante i slike drøftinger.

[8] Oppdrags- og bestillingsdokument - Helse Sør-Øst RHF

  - Fastsette overordnet mål og strategi for informasjonssikkerhet i Helse Sør-Øst.
  - Fastsette overordnet mål og strategi for personvern i Helse Sør-Øst.
  - Tilrettelegge for samarbeid mellom informasjonssikkerhetslederne ved helseforetakene og det regionale helseforetaket, blant annet gjennom regionalt sikkerhetsfaglig råd (RSR).
  - Tilrettelegge for samarbeid mellom personvernfagmiljøene ved helseforetakene og det regionale helseforetaket, blant annet gjennom et regionalt personvernråd.
  - Tilrettelegge for helhetlig og effektiv vurdering og håndtering av risiko innen informasjonssikkerhetsområdet i foretaksgruppen.
  - Stille krav til informasjonssikkerhet og personvern i nasjonale og regionale anskaffelser, herunder avtaler med private sykehus.
- Ha oversikt over personvern- og informasjonssikkerhetstilstanden og de største risikoer i foretaksgruppen.
- Delta i samarbeid mellom regionene på personvern- og informasjonssikkerhetsområdet.
- Sørge for at det finnes et konsernfelles personvernombud og at dette kan ivareta lovpålagte krav, herunder at helseforetakene har enkel tilgang til ombudet.
- Sørge for egnete felles møteplasser mellom konsernfelles personvernombud og helseforetakene (herunder fagressurser og ledere).

3.3 Sykehuspartner

Sykehuspartner har ansvar som leverandør og databehandler i henhold til avtaler med helseforetakene, og for øvrig ansvar som helseforetak og dataansvarlig, jf. punkt 3.1.

Sykehuspartner skal:

- Sørge for egnet sikkerhet i infrastrukturen i Helse Sør-Øst[9]. Ved usikkerhet om hvorvidt et tiltak er sikkerhetsmessig lønnsomt skal risikovurderingen legges fram for representanter fra helseforetakene til drøfting.
- Ivareta informasjonssikkerheten som databehandler i henhold til avtaler og regelverk, herunder krav til internkontroll og avvikshåndtering. Være foretaksgruppens kompetansemiljø for informasjonssikkerhet.
- Understøtte helseforetakenes internkontrollarbeid på informasjonssikkerhets- og personvernområdet, herunder utarbeide presiserende og utfyllende dokumenter i ledelsessystemet.
- Utføre og drive prosesser for risikovurderinger, både for infrastruktur og tjenester iht. avtale med helseforetakene.
- Bidra til utforming av sikkerhetskrav i anskaffelser.
- Kunne stille bruksvilkår innenfor de rammene som er satt regionalt.[10]
- Være foretaksgruppens responsmiljø for hendelser (CERT) og Sykehuspartner skal kunne ta ned tjenester i henhold til avtaler.[11]

[9] Styresak 004-2020 vedlegg 5, jf. protokoll 5. februar 2020.

[10] Styresak 107-2019 s 9, jf. protokoll 19. desember 2019 pkt 2.

[11] Styresak 077-2017, jf. protokoll 28. juni 2017 pkt 5.

4 Roller i helseforetaket

Organisering av informasjonssikkerhetsarbeidet avklarer nødvendige ansvars- og myndighetsforhold og omfatter utøvende og kontrollerende ansvar og oppgaver, herunder utpeking av hvilken risiko hver rolle er ansvarlig for (er risikoeier for).

Risikoeiere skal innen sitt ansvarsområde håndtere usikkerhet knyttet til måloppnåelse. Risikoeiere må vurdere og akseptere risikoen for at mål ikke nås, både når det gjelder helseområdet, personvern-området og etterlevelse av øvrig regelverk. I dette ligger også krav om egnet informasjonssikkerhet.

Hva som er høyeste restrisikonivå som den enkelte rolle kan akseptere, er fastsatt i NO-5[12], ev. med tilpasninger fra helseforetaket.

4.1 Administrerende direktør

Administrerende direktør

- er risikoeier for helseforetakets samlede måloppnåelse
- har det overordnede ansvar for egnet informasjonssikkerhet og godt personvern
- er ansvarlig for å påse at helseforetaket har et effektivt internkontrollsystem på personvern- og informasjonssikkerhetsområdet, herunder at:
    - Internkontrollsystemet er tilpasset risiko, vesentlighet og egenart.
    - Det eksisterer overordnede føringer og prinsipper med tilhørende definert myndighet, roller og ansvar knyttet til helseforetakets vesentlige og risikoutsatte områder, og at dette er dokumentert i policyer.
    - Systemet er innrettet slik at det bidrar til at helseforetaket når de mål som er fastsatt, gjennom en målrettet og effektiv drift, pålitelig rapportering og overholdelse av lover og regler.
    - Varsling ved informasjonssikkerhets- og personvernbrudd til Helsetilsynet, Datatilsynet, Nasjonal sikkerhetsmyndighet og eventuelt andre utføres i henhold til krav i regelverket.

4.2 Systemeier

Systemeier er risikoeier for at systemet har egnet informasjonssikkerhet og personvern. Beskrivelsen gjelder også for regionale systemeiere i Helse Sør-Øst RHF.

- Systemeier er ansvarlig for at et system utvikles, forvaltes og driftes. Systemeier skal
    - inngå i endringsstyringsprosessen hos IKT-leverandør/databehandler og beslutte gjennomføring av endringer for sitt system
    - sørge for at det kan gis nødvendig opplæring for å kunne benytte systemet på korrekt måte
    - overvåke risiko forbundet med informasjonsbehandling og forestå risikovurdering ved behov
- Systemeier skal sørge for at systemet har egnet informasjonssikkerhet. Systemeier skal
    - sørge for at systemet har logging, tilgangsstyring og etterfølgende kontroll, i samsvar med regionale prinsipper for tilgang.
    - bistå foretaket i kontinuitetsplanlegging for arbeidsprosesser der systemet inngår

[12] NO-5 - Kriterier for vurdering og aksept av risiko for informasjonssikkerhet

- Systemeier skal sørge for at systemer oppfyller krav iht. personvernforordningen, herunder
  - at det foreligger skriftlige avtaler (databehandleravtale) med IKT-leverandør/data-behandler, jf. pvf art 28 nr 3
  - etterlevelse av krav til innebygd personvern og personvern som standardinnstilling, jf. pvf art 25
  - etterlevelse av krav til at personvernkonsekvensvurdering (DPIA) gjennomføres (ved sannsynlig høy risiko for de registrerte), jf. pvf art 35
- Systemeier skal dessuten følge krav i helseforetakets funksjonsbeskrivelse for rollen, dersom slik er utarbeidet, jf. kapittel 3.1.

4.3 Informasjonssikkerhetssleder

Informasjonssikkerhetsleder skal

- ha rett til å eskalere informasjonssikkerhetsspørsmål i linjen og direkte til administrerende direktør for helseforetaket, eksempelvis ved behov for nye/endrede sikkerhetstiltak eller tvil om hvorvidt en restrisiko er riktig beskrevet og håndtert
- være en ressursperson, pådriver og tilrettelegger for etablering og gjennomføring av helseforetakets samlede internkontroll innen informasjonssikkerhet. Til rollen hører blant annet å:
  - Lage revisjonsplaner og sikre gjennomføring av sikkerhetsrevisjoner i helseforetaket, samt rapportere planer og resultater gjennom helseforetakets etablerte kanaler for øvrig revisjonsaktivitet.
  - Vurdere og følge opp på rapporterte avvik og meddele avvik til virksomhetens ledelse i samsvar med helseforetakets etablerte rutiner for avviksbehandling.
  - Drive opplysningsvirksomhet i foretaket om informasjonssikkerhet.
  - Utvikle og vedlikeholde overordnede styrende dokumenter innen ansvarsområdet.
  - Være til støtte i gjennomføring av risikovurderinger.
  - Delta i regionale fora for informasjonssikkerhet.
- støtte virksomhetsledelsen i spørsmål om informasjonssikkerhet, herunder
  - ha ansvar for faglig rapportering til helseforetakets ledelse innen sitt fagområde
  - forberede ledelsens årlige gjennomgang av bruk av informasjonssystemet
- kunne akseptere lav restrisiko i henhold til akseptkriteriene[13]
- følge krav i helseforetakets funksjonsbeskrivelse for rollen

4.4 Personvernleder

Personvernleder skal

- ha rett til å eskalere personvernspørsmål i linjen og direkte til administrerende direktør for helseforetaket, eksempelvis ved behov for nye/endrede personverntiltak eller tvil om hvorvidt en restrisiko er riktig beskrevet og håndtert
- være en ressursperson, pådriver og tilrettelegger for etablering og gjennomføring av helseforetakets samlede internkontroll innen personvern. Til rollen hører blant annet å:
  - Bidra til kontroller av virksomhetens arbeid med personvern i linja, herunder relevante deler av virksomhetens internkontrollsystem. Rapportere planer og resultater gjennom helseforetakets etablerte kanaler for øvrig revisjonsaktivitet.

[13] NO-5 - Kriterier for vurdering og aksept av risiko for informasjonssikkerhet

  - Bidra til tilstrekkelig kunnskap om store risikoer og sårbarheter på personvernområdet, herunder, tilrettelegge for oppfølging av rapporterte avvik og meddele avvik til virksomhetens ledelse i samsvar med helseforetakets etablerte rutiner for avviksbehandling.
  - Drive opplysningsvirksomhet i foretaket om personvern.
  - Utvikle og vedlikeholde overordnede styrende dokumenter innen ansvarsområdet.
  - Rådgi og støtte linja til å gjennomføre personvernvurderinger og personvernkonsekvensvurderinger.
  - Delta i regionale fora for personvern.
- støtte virksomhetsledelsen i spørsmål om personvern, herunder
  - ha ansvar for faglig rapportering til helseforetakets ledelse innen sitt fagområde
  - forberede ledelsens årlige gjennomgang av personvernområdet
- følge krav i helseforetakets funksjonsbeskrivelse for rollen

4.5 Uavhengig personvernrådgiver for forskning

Helseforetakene som utfører forskning som omfattes av personopplysningsloven §§ 9 og 10 skal etterleve den særnorske rådføringsplikten innen forskningsområdet, jamfør nevnte bestemmelser, ved bruk av alternativet rådføring med «en annen» kvalifisert og uavhengig rådgiver.

4.6 Konsernfelles personvernombud

Personvernombudet rapporterer direkte til øverste ledelse i helseforetakene, jf. pvf artikkel 38 nr 3 siste punktum. I henhold til helseforetaksloven er øverste ledelse styret og daglig leder.

Personvernombudet skal bistå de dataansvarlige og databehandlerne i å kontrollere etterlevelsen av forordningen, jf. pvf fortalepunkt 97.

Personvernombudet skal ivareta lovpålagte oppgaver, herunder:

- Informere og gi råd om personvernforpliktelser
- Kontrollere overholdelse av personvernforpliktelser, herunder gjennomføringen av personvernkonsekvensutredninger
- På anmodning gi råd om vurderinger av personvernkonsekvenser
- Være kontaktpunkt for de registrerte.
- Samarbeide med og være kontaktpunkt for Datatilsynet, herunder rådføre seg med tilsynet ved behov og være kontaktpunkt ved forhåndsdrøftinger.

Personvernombudet skal ved utførelsen av sine oppgaver ta behørig hensyn til risikoene forbundet med behandlingsaktivitetene, idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, jf. artikkel 39 nr 2.

Personvernombudet skal i utgangspunktet ikke pålegges andre oppgaver enn de lovpålagte. Andre plikter, eksempelvis knyttet til rapportering, kan kun pålegges etter avtale med Helse Sør-Øst RHF. Helseforetakene og Helse Sør-Øst RHF må påse at ombudet ikke pålegges oppgaver eller plikter som fører til en interessekonflikt, jf. pvf artikkel 38 nr 6.

4.7 Leder

Leder er risikoeier for måloppnåelsen innen sitt ansvarsområde i samsvar med fastsatte rammer[14].

Ansvaret dekker blant annet å ha tilstrekkelig kontroll med informasjonen og egen, ansattes og underleverandørers bruk av informasjonssystemer i utførelse av arbeidsoppgaver.

Leder skal sørge for at det daglige *informasjonssikkerhetsarbeidet* følges opp innen sitt ansvarsområde, herunder å sørge for at

- informasjonsbehandlingen har egnet informasjonssikkerhet, herunder at risiko knyttet til bortfall av IKT-systemer er vurdert
- eget og innleid personell har tilstrekkelig sikkerhetskompetanse og forståelse av hva som er forventet av dem. Kjennskap til sikkerhetsinstruksens innhold er et minimumskrav.
- tilgangsstyringen er egnet, herunder at
    - eget og innleid personell får tilgang til informasjon ved behov
    - informasjon er tilstrekkelig skjermet for uberettiget innsyn
    - informasjon er tilstrekkelig beskyttet mot utilsiktet eller uberettiget endring
- uønskede hendelser og informasjonssikkerhetsbrudd følges opp

Leder skal sørge for at det daglige *personvernarbeidet* følges opp innen sitt ansvarsområde, herunder å sørge for at

- personvernkonsekvensvurdering (DPIA) gjennomføres dersom leder beslutter ny eller endret behandling av personopplysninger, som sannsynligvis vil innebære høy risiko for de registrerte
- krav til at personopplysningene behandles med tilstrekkelig rettslig grunnlag, kvalitet og omfang (inkl. dataminimering), og at informasjonsplikt til de registrerte mv., etterleves

Ledere på alle nivåer skal minst en gang årlig *vurdere status* innen eget ansvarsområde, om leder har tilstrekkelig kontroll med informasjonssikkerhets- og personvernrisikoen på sitt ansvarsområde.

Ledere på alle nivåer har ansvar for oppfylling av dokumentet i egen enhet.

4.8 Medarbeider

Den enkelte medarbeider er ansvarlig for å løse arbeidsoppgavene effektivt og bruke informasjon aktivt. Dette skal skje med egnet informasjonssikkerhet og godt personvern. I dette ligger

- å følge helseforetakets sikkerhetsinstruks og andre sikkerhetsbestemmelser
- å ha en forståelse av hva som er forventet av dem (adferd). For medarbeidere som skal ha tilgang til taushetsbelagte opplysninger, skal også grunnlag og hjemmel for oppslag i de taushetsbelagte opplysningene være forstått
- å søke informasjon ved usikkerhet eller tvil
- å rapportere uønskede hendelser, avvik og informasjonssikkerhetsbrudd i henhold til helseforetakets avviksrutiner

[14] Blant annet Kriterier for vurdering og aksept av risiko for informasjonssikkerhet (NO-5).