ORIENTERINGSSAK

Til:	Møtedato:	Sak:
Fakultetsstyret for Det helsevitenskapelige fakultet		

Behandling av årsrapport for informasjonssikkerhet

Forslag til Vedtak:
Årsrapport for informasjonssikkerhet tas til orientering.

Bakgrunn:
I juli 2018 trådte bestemmelsene i personopplysningsloven og EUs personvernforordningen (General data protection regulation – GDPR) i kraft. Med personvernforordningen flyttet lovgiver ansvaret for personvernet fra Datatilsynet til den enkelte virksomheten. Ved innføringen av personvernforordningen fikk UIT dermed et utvidet ansvar for å sørge for at behandling av personopplysninger skjer i samsvar med de lov og forskriftskrav som gjelder.

For UiTs del omfattes all vår behandling av personopplysninger av personvernforordningen. Eksempelvis gjelder personvernforordningen for den behandlingen av personopplysninger som det helsevitenskaplige fakultet gjør i de ulike forskningsprosjektene, de store befolkningsundersøkelsene, studentoppgavene, i forbindelse med arrangementer, og om UiTs ansatte og studenter.

I personvernforordningens andre avsnitt stilles det krav til personopplysningssikkerheten. I tillegg har UiT ansvar for å jobbe med informasjonssikkerhet knyttet til opplysninger som ikke kan defineres som personopplysninger. Dette kan eksempelvis være opplysninger av sikkerhetsmessig eller økonomisk art. I det følgende blir begrepet informasjonssikkerhet brukt om både personopplysningssikkerhet og annen informasjonssikkerhet.

Avdeling for IT (ITA) har utarbeidet en årsrapport for 2019 som belyser ulike utfordringer som også gjør seg gjeldende for Helsefak. Årsrapporten for 2019 omhandler kun informasjonssikkerhet, øvrige utfordringer knyttet til arbeidet med personvern vil først bli tatt inn i årsrapporten for 2021.

Årsrapporten for informasjonssikkerhet 2019 ble behandlet av universitetsstyret den 5 mars 2020. Universitetsstyret fattet to vedtak (Sak S 10/20):

> *1. Universitetsstyret tar årsrapporten for Informasjonssikkerhet (2019) til etterretning og ber om at arbeidet med informasjonssikkerhet ved UIT styrkes.*

2. Styret ber om at årsrapporten tas opp i alle fakultetsstyrer og styrer for Universitetsbiblioteket og Norges arktiske universitetsmuseum og akademi for kunstfag.

Som en del av oppfølgingen av Universitetsstyrets vedtak tas saken nå opp for Fakultetsstyret.

Vurdering
Årsrapporten er lagt ved, og i det følgende vil de delene av rapporten som har særlig betydning for Helsefak bli trukket frem.

Fokus hos ledelsen
Universitetsdirektøren har det overordnede ansvaret for informasjonssikkerheten. IT-direktøren har forvaltningsansvaret for informasjonssikkerhet, mens enhetsledere (Dekaner og avdelingsdirektører) er ansvarlige for å tilfredsstille krav til informasjonssikkerhet i egne enheter, jf. Årsrapportens pkt. 5. Dette innebærer at det daglige ansvaret for å etterleve kravene som stilles til informasjonssikkerhet ligger på fakultetet selv.

I årsrapporten pekes det på at det er behov for å styrke oppmerksomheten og kompetansen i ledelseslinjen på UiT, og at det er viktig at ledelsen ved UiT har tilstrekkelig fokus på informasjonssikkerhet. Av årsrapporten går det frem at det derfor er viktig at informasjonssikkerhet tas opp som eget tema i ledermøtene på fakultetet. Helsefak støtter dette, og ønsker å løfte informasjonssikkerhet og personvern som tema på ledermøtene minst en gang i året. Ved å sette fokus på informasjonssikkerhet i ledermøtene vil det være lettere å lage en overordnet strategi for informasjonssikkerhet og personvern på fakultetet, samt orientere om evt avvik og pågående arbeid med disse temaene på fakultetsnivå.

Avvikshåndtering
ITA har ansvar for oppfølgning av avvik knyttet til informasjonssikkerhet. ITA mottok i 2019 melding om 20 avvik, noe som er lavt for en organisasjon som UiT. I årsrapporten utrykkes det en bekymring for underrapportering av avvik som følge av at manglende kompetanse og oppmerksomhet på hva som skal meldes som avvik. Som eksempel nevnes at mange av de innmeldte avvikene ikke blir meldt gjennom UiTs system for avviksmeldinger, men blir oppdaget gjennom andre kanaler som brukerstøtte, noe som igjen kan indikere at ansatte på UiT i for liten grad har bevissthet og kunnskap om hvordan avvik meldes.

På Helsefak behandler de ansatte store mengder opplysninger daglig, herunder sensitive personopplysninger. Det kan eksempelvis være snakk om opplysninger om ansatte ved UiT, opplysninger om forskningsdeltakere eller opplysninger om forskningsprosjekter. Avvikshåndtering er en viktig del av Internkontrollsystemet ved UiT og gir ledere en mulighet til å bli kjent med mulige risikoer knyttet til virksomheten. Samtidig er det et eget avvikssystem knyttet til avvik etter helseforskningsloven. Disse avvikene overlapper ofte med avvik om informasjonssikkerhet eller personvern for øvrig, og det kan være vanskelig for å den enkelte ansatte å vite hvor et avvik skal meldes. Fakultetet ønsker derfor å jobbe med ITA for å samkjøre de forskjellige avvikssystemene, slik at ledere og ansatte kun trenger å forholde seg til et system. Det er verdt å nevne at også etter helseforskningsloven, meldes det ikke fra om avvik på fakultetet.

For å kunne ivareta ansvaret for informasjonssikkerheten i enheten, og for å kunne forebygge mulige avvik er det avgjørende at avvik meldes rutinemessig fra alle ansatte ved fakultetet.

Mangelfull avviksrapportering reduserer fakultetets mulighet til å rette mangler i den daglige driften, eksempelvis gjennom rutineendringer, før nye mulige avvik oppstår. Manglende avviksrapportering vil også kunne gjøre det vanskelig for UiT å sette i gang tiltak som kan redusere skadevirkninger av avvik som har oppstått.

For Helsefak er det viktig at ledere setter søkelys på kompetanse omkring avvikssystemet og på god meldekultur herunder at ansatte melder fra om avvik som oppstår i den daglige driften av fakultet.

For de avvikene som er meldt er det kun de fem mest alvorlige avvikene som er behandlet i årsrapporten. Helsefak har ingen oversikt over totaliteten av avvik og det er derfor vanskelig å bedømme hvorvidt det er andre avvik som foreligger på fakultetet. Av de fem som er nevnt tilhører tre av avvikene Helsefak, mens de to øvrige avvikene er tilfeller som er på flere fakultet uten at det er nevnt særskilt hvilke fakultet de gjelder. Da kun et fåtall av meldte avvik fremkommer av årsrapporten er det vanskelig å finne fellestrekk som kan styre fakultetets arbeid med informasjonssikkerhet

Bruk av video
I årsrapporten fremheves det video er i utstrakt bruk på UiT, og at det er lett å trå galt ved bruk av video. Bruk av video har stort skadepotensiale, og for de som blir filmet vil det kunne oppleves særlig inngripende og krenkende. Det påpekes at studenters bruk av video i studiet, ved eksempelvis datainnsamlinger er særlig risikofylt ettersom det da ofte benyttes privat utstyr.

Ved Helsefak er bruk av video vanlig, og brukes i økt grad nå som følge av mer digitalisering ved Covid-19. For eksempel brukes video til opptak av forelesninger, konferanser, veiledning, eksterne sesjoner, utdanning forskning med mer. Video benyttes også i reelle pasientkonsultasjoner og til datainnsamlinger, noe som innebærer at innholdet som filmes ved fakultetet kan være svært sensitivt, og ha stort skadepotensiale dersom UiT ikke har kontroll på hvordan opplysningene på video behandles. Eksempelvis kan man se for seg at studenter har sensitive opptak på sin mobil eller pc når de slutter ved UiT, uten at UiT har kontroll på disse opplysningene. Det kan også tenkes at ansatte lagrer videoer på en måte som ikke tilfredsstiller kravene til informasjonssikkerhet for eksempel ved bruk av skytjenester som ikke er godkjent for slik bruk.

Når det gjelder studenters bruk av privat utstyr har UiT og Helsefak klare retningslinjer som gjør det klart at studenter ikke kan benytte privat utstyr som mobil og pc som verktøy til eksempelvis datainnsamling for masteroppgaver og arbeidskrav. Det er likevel slik at UiT per i dag ikke har et godt alternativ å tilby studentene for lagring av slikt materiale da det ikke er mulig å tilby alle studenter utstyr som eies av UiT, og det eneste alternativet for studenten i dag er å benytte krypterte minnepenner som tilhører universitetet. Dette innebærer igjen er stor risiko ved at informasjonen lagret på minnepennen går tapt, dersom studenten mister eller ødelegger minnepennen. Helsefak mener derfor at det er en stor risiko for at privat utstyr blir benyttet i betydelig grad av studenter.

Av oversikten over avvik i 2019 fremgår det også at flere enheter, inkludert Helsefak, hadde avvik knyttet til bruk av privat utsyr.

ITA har i sin årsrapport fremhevet at de ulike enhetene må ha personer som kan ta vurderinger knyttet til bruk av video fortløpende og effektivt. På Helsefak kan denne typen henvendelser rettes til juristene i fakultetsadministrasjonen.

Risikovurderinger
Innenfor informasjonssikkerhet er risikostyring viktig. Gjennom systematisk kartlegging av potensielle risikoer vil man kunne igangsette tiltak for å redusere risikoen som man måtte avdekke.

Risikovurderinger skal gjennomføres

- Når trusselbildet endres
- Før oppstart av behandling av personopplysninger
- Ved oppstart av forskningsprosjekter uridisk seniorrådgiver
- Ved etablering eller endring av IKT- systemer
- Ved organisatoriske endringer som kan påvirke informasjonssikkerheten.

I årsrapporten fremgår det at det er en bedring i antallet risikovurderinger som gjennomføres ved UiT, men at det fremdeles er en lang vei å gå. Faggruppen for personvern ved ITA har endret sitt fokus fra aktiv deltakelse i risikovurderinger til rådgivning innenfor risikovurderinger. Det innebærer at fakultetet selv er ansvarlig for at det gjennomføres risikovurderinger i tilfeller hvor dette er nødvendig.

Fakultetet har per i dag ikke avsatt ressurser for arbeid med risikovurderinger og det er ingen ansatte som har dette som del av sine oppgaver. Så vidt fakultetet er kjent med, er det instituttene selv som gjennomfører risikovurderinger for sine prosjekt. Det er heller ingen på fakultetet som har oversikt over hvor mange risikovurderinger som er gjennomført. Det finnes imidlertid en oversikt over risikovurderinger hos ITA. Denne oversikten er nylig opprettet (2020) og er derfor ikke en komplett historisk oversikt. På denne oversikten er Helsefak oppført med fire risikovurderinger, noe som vurderes å være lite når man ser på oversikten over når det skal gjennomføres risikovurderinger. For eksempel skal det gjennomføres risikovurderinger i alle forskningsprosjekter som gjennomføres ved Helsefak. Det må kunne antas at det er gjennomført flere risikovurderinger enn det som kommer frem av oversikten til ITA, men det er ikke mulig å hente ut en komplett oversikt for å underbygge dette.

Den manglende oversikten er utfordrende for Helsefak da fakultetet årlig blant annet skal rapportere om status på risikovurderinger.

Det kan ikke forventes at alle ansatte besitter kompetanse om gjennomføring av risikovurderinger, men fakultetet må sikre at man har ansatte som kan bistå med rådgivning. Fakultetet har i dag ikke ansatte med særlig kompetanse innen risikovurderinger, og det må sørges for at flere ansatte i administrasjonen har denne kompetansen. Det vil være naturlig at denne kompetansen bygges opp på Prosjektkontoret etter hvert.

Årlig statusrapport
I 2019 ble det innført en årlig statusrapport som de ulike enhetene skal levere. I rapporten skal Helsefak kartlegge informasjonsverdiene sine, identifisere sårbarheter, vurdere trusler og tiltak, orientere om status på risikovurderinger og organiseringen av arbeidet ved fakultetet. Arbeidet med statusrapportering er utfordrende da fakultetet ikke i dag har dedikerte ansatte som jobber

med informasjonssikkerhet. Det er derfor ikke etablert gode rutiner og oversikter på fakultetet som lett kan benyttes ved statusrapporteringen. Det er eksempelvis ingen oversikt over hvilke avvik som er meldt eller hvilke risikovurderinger som er gjennomført da disse oversiktene per i dag ligger på ITA men disse vil kun inneholde risikovurderinger utført etter januar 2020. Helsefak vil samarbeide tettere med ITA for å avklare hvilke elementer som skal ivaretas av ITA selv og av fakultetet, for å forhindre dobbeltarbeid og kontroll på flere enheter.

Konklusjon

Fakultetsdirektør og dekan har ansvaret for å ivareta informasjonssikkerheten i sin enhet. For å kunne lykkes i dette arbeidet må man sørge for at lederlinjen har tilstrekkelig søkelys på informasjonssikkerhet. Lederlinjen må videre sørge for at ansatte har tilstrekkelig kompetanse om de rutiner og retningslinjer som finnes og at disse følges i praksis. Fremover bør det settes av ressurser som har kompetanse på informasjonssikkerhet og som kan ivareta oppgavene som nå er tillagt fakultetet, herunder statusrapportering, risikovurdering, avvikshåndtering og generell rådgivning. Selv om enkelte av disse elementene i dag ivaretas av andre (enhetsledere, forskere og jurister i fakultetsadministrasjon), er det ingen som har en konkret rolle i dette arbeidet i dag.

Thrina Loennechen
Dekan
–

Trond Nylund
Assisterende fakultetsdirektør
–

Dokumentet er elektronisk godkjent og krever ikke signatur

Saksbehandlere: Jannicke Persen og juridisk seniorrådgiver Frank Tore Mengkrogen

Vedlegg
1 Årsrapport for informasjonssikkerhet 2019