



## Statusrapport fra personvernombudet ved KHIO

**SAK:** Status Personvern KHIO

**TEMA:** Status på personvern og informasjonssikkerhet hos KHIO.

**DATO:** 28. februar 2020

**TIL:** Behandlingsansvarlig Annemarie Bechmann Hansen,  
SCO Pål Stephensen og ISR Geir Hamre Moe

**FRA:** Rolf Haavik, personvernombud (PVO) for KHIO

### Innledning

Dette er personvernombudets oppsummering av status på arbeidet med informasjonssikkerhet og personvern i KHIO etter de fire første måneder som personvernombud.

Jeg har naturlig nok ikke fått inngående kjennskap til status på informasjonssikkerhet på denne korte tiden. Jeg har jobbet en del med Teamleder IT og hatt noen innledende møter med styret og ledelse.

Fokus den første tiden har vært på administrasjonen ved KHIO. Det har også vært noe kontakt med de faglige miljøene i forbindelse med vurdering av personvern i to masteroppgaver. Og det har også vært noen spørsmål fra ansatte om ulike personvernforhold er mottatt og behandlet.

### Ledelsessystem for Informasjonssikkerhet (LSIS)

#### Holdninger

Gjennom den kontakten jeg har hatt med ledelsen ved KHIO er mitt inntrykk at de gir personvern høy prioritet. Bevisstheten rundt personvern og informasjonssikkerhet i organisasjonen for øvrig er imidlertid variabel, viser svarene på Nano-læringen som er gjennomført. Noen grupper peker seg ut som trenger bedre forståelse, mens andre grupper scorer bra.

Holdningsskapende arbeid rundt personvern og informasjonssikkerhet er veldig viktig. Ledelsen har en viktig rolle her.

#### Styrende dokumenter

Styrende dokumenter er basert på en eldre mal fra Uninett, som hovedsakelig har tatt sitt utgangspunkt i ISO 27001. Dokumentene trenger en oppdatering etter GDPR, slik at sentrale begrep i ny personopplysningslov dekkes i større grad. Beskrivelser av rollene bør detaljeres både for administrative og faglig avdelinger.

#### Sikkerhetsorganisasjonen og ansvar

Et hovedgrep som er gjort er at det operative ansvaret for personvern og informasjonssikkerhet er løftet til seksjons- og instituttledernivå. Seksjons- og instituttledere med operativt ansvar for et behandlingsområde (systemeier) vil være ansvarlig for personvern og sikkerhet for all informasjon

innen sitt område. Informasjon kan eksistere i IKT-systemer, på filområder, på intranett, i epost og annen informasjonslagring, -deling og -oversending.

Det er innført en ny rådgivende rolle som Informasjonssikkerhetsrådgiver (ISR). Denne rollen eksisterte ikke tidligere, kun CSO. Vi er i en overgangsperiode frem til alle systemeiere har fått tilstrekkelig opplæring, hvor ISR gradvis overleverer deler av ansvaret for personvern til systemeiere.

## Motivasjon og opplæring

Det bør gjennomføres opplæring i informasjonssikkerhet og personvern for alle ansatte og for systemeiere spesielt. Det bør lage veiledninger som setter alle systemeiere i stand til å utføre de pålagte oppgaver som risikovurdering, vedlikehold av protokoll, nye behandling, sletting mm.

Gjennomføring av risikovurderingen med systemeiere vil også være et nyttig bidrag i opplæring, på hvordan man tenker sårbarhet, risiko og tiltak innen personvern.

Opplæringsplaner bør etableres og holdes løpende oppdatert. On-boarding rutiner for nyansatte kan gjerne inkludere en samtale med ISR om personvern.

## Avviksmelding og avvikshåndtering

Avviksrapportering er innarbeidet som en del av den operative delen av ledelsessystemet i Agora. Det benyttes imidlertid lite og bør gjøres mer brukervennlig.

## Sikkerhetsrevisjon og egenkontroll

UNIT hadde en gjennomgang på KHiO 12. februar, endelig rapport er ikke fremlagt enda.

Denne rapport kan ses på som en egenkontroll.

## Risikovurderinger

Risikovurderinger blir gjennomført, hovedsakelig av ISR, men det er et fåtall tiltak som kommer ut av dette. For å få god effekt, må alle systemeiere delta aktivt i risikovurderingene, og det er deres ansvar å gjennomføre regelmessig. For å få til dette må metoden for risikovurdering revideres og det må gjennomføres opplæring i risikovurdering, gjerne med deltakelse av ISR eller PVO de første ganger.

Risikovurderinger gjennomføres ikke systematisk i IT-prosjekter eller anskaffelser. Det bør utarbeides en kort prosjekthåndbok som beskriver hvordan prosjekter skal gjennomføres med minstekrav til innebygget personvern og risikovurdering. Det er meget god økonomi i å få godt personvern levert i første versjon, i forhold til å måtte bestille endringer i etterkant av leveransen.

## Beredskap

Det er gjennomført en beredskapsøvelse med tema personopplysninger på avveie.

## Kartlegging av informasjonsverdier

Det er gjennomført kartlegging i henhold til Uninett sin mal for alle behandlinger av personopplysninger.

Protokoll finnes for administrative system, men ikke samlet i et dokument eller system og er derfor ikke lett tilgjengelig. Formelt sett ikke noe galt i det, men på sikt bør protokollen inn på et dokument (eller helst et verktøy).

KHiO bør vurdere å ta i bruk NSD sitt Meldingsarkiv, som er et meget godt verktøy for å planlegge og følge opp gjennomføring av forskningsprosjekt. Her er også en veileder som viser informasjon om

begreper, forklaringer og tilbyr maler på ulike områder. NSD vurderer prosjektet og kommer tilbake med et svar med anbefalinger. Og det er en meget god protokoll.

Det er innhentet databehandleravtale fra alle aktuelle leverandører (databehandleravtaler).

Rutiner for ny behandling står på agenda for fellesmøte i januar.

## Lagring og sletting

Mye er på plass når det gjelder sletting, men fellesområder er en utfordring.

Tiltak på lagring og sletting bør være:

1. Å definere lagrings- og slettepolicy for alle behandlinger. Hvor lenge har KHIO lov til å behandle personopplysningene?
2. Beskrive hvordan man sletter personopplysninger som skal slettes? Rutiner for sletting bør utarbeides.
3. Når en slettepolicy er etablert skal sletting av personopplysninger gjennomføres.

Anonymisering har samme effekt som fysisk sletting. Man beholder da statistikker og anonymisering er lettere (og mindre kostbart) å få til enn sletting. Mange leverandører leverer anonymisering når man ber om sletting.

Krav til sletting gjelder på alle lagringsformater, i strukturerte IKT-systemer, på filområder, i e-post, i papirarkiv, på Internett, Teams, mm.

## Innsyn

Rutiner for behandling av innsynsbegjæringer av personopplysninger er utarbeidet, men ikke ferdig tilpasset til KHIO enda. Dette arbeidet står i handlingsplanen og må prioriteres nå.

## Personvernerklæringer

Det er utarbeidet meget gode personvernerklæringer for ansatte for SAP og studenter for FS og tilhørende systemer. Det er løpende oppdatering av personvernerklæringer også for andre systemer.

## Teknisk informasjonssikkerhet

Sikring av personopplysninger mot eksterne trusler er et veldig viktig aspekt av GDPR.

Sikkerhetsanalyse og logganalyse leveres fra Uninett.

Det er behov for økt sikkerhet rundt informasjon på usikrede enheter. Dette er et tema på samlingen for ISR i de fire samarbeidende høyskoler, med bistand fra UNIT eller UNINETT.

## Kontinuerlig forbedring

De fleste tiltak nevnt i denne rapport krever løpende oppfølging, og årshjul og handlingsplaner må implementeres slik at tiltak ikke blir en en-gangs øvelse.

- Det er etablert styrende dokument, nye veiledere og nye rutiner. Disse krever årlig evaluering og oppdatering, fungerer det etter hensikten?
- Risikovurdering er gjennomført, men nye risiko kommer stadig. Risikovurderingen bør regelmessig oppdateres, handlingsplaner gjennomgås og tiltak evalueres.
- Opplæring i personvern og informasjonssikkerhet må repeteres for alle og nye ansatte må få full opplæring i personvern ved KHIO.

## Synergier fra PVO arbeidet

Det er et mål å trekke ut synergier i arbeidet med informasjonssikkerhet og personvern for de 4 høyskoler. Synergier oppnås på følgende måter:

1. Gjennom utarbeidelse av nye rutiner og maler i samarbeidsforum for ISR. Vi gjennomførte første møte i dette forum i januar og neste møte er 10 januar med en rekke punkter med felles interesse på agendaen.
2. Få veiledning og kompetansebygging på områder som ikke er lett å få oversikt over. Vi planlegger en workshop med UNIT eller Uninett om sikring av informasjon på PC'er, Mac'er og bærbare enheter
3. PVO formidler gode idéer og gode felles løsninger mellom høyskolene i sitt virke.
4. PVO deltar på forum for personvernombud for de fire høyskoler, og deler presentasjons materiale. Sparer tid og penger.