UiO : Universitetet i Oslo
Universitetsdirektøren

**Til** **Universitetsstyret**
**Fra** **Universitetsdirektøren**

| | |
|---|---|
| **Sakstype:** | **Orienteringssak** |
| **Møtesaksnr.:** | **O-sak 2** |
| **Møtenr.:** | **3/2020** |
| **Møtedato:** | **5. mai 2020** |
| **Notatdato:** | **8. april 2020** |
| **Arkivsaksnr.:** | |
| **Saksbehandler:** | **Espen Grøndahl, Martin Bore, Vilde Sørbø Nenseth** |

# Status på arbeidet med informasjonssikkerhet og personvern ved Universitetet i Oslo

Kunnskapsdepartementets styringsmodell for informasjonssikkerhet i høyere utdanning og forskning spesifiserer styrets ansvar for informasjonssikkerhet og personvern. I denne saken orienteres det om UiOs arbeid på områdene.

Det vises også til tidligere orienteringer i styret 7. mai 2o19 «Status på arbeidet med informasjonssikkerhet og personvern ved Universitetet i Oslo».

## Hovedproblemstillinger i saken

Fokuset på informasjonssikkerhet og personvern har økt de siste årene. Informasjonssikkerhet er utfordrende på et universitet hvor man ønsker åpenhet, samarbeid med andre forskere i inn- og utlandet samtidig som man skal benytte IT-løsninger som beskytter UiOs verdier. Det er nye og tydeligere krav til informasjonssikkerhetsarbeidet i lov- og regelverk, i tildelingsbrev, digitaliseringsstrategi mv. Og det er et sterkt økende internasjonalt trusselbilde. Svikt i informasjonssikkerhetsarbeidet kan medføre store konsekvenser for UiO, både økonomisk og omdømmemessig.

I denne saken orienteres styret om følgende:

- Digitalisering
- Policy for informasjonssikkerhet
- Eksportkontroll
- Ledelsessystem for informasjonssikkerhet
- Personvern i forskning
- Internkontroll
- Trusselbildet
- Videre arbeid

Arne Benjaminsen
universitetsdirektør

Lars Oftedal
IT-direktør

---

Vedlegg:

- Fremleggsnotat med tilhørende vedlegg

UiO : Universitetet i Oslo

FRA
UNIVERSITETSDIREKTØREN

FREMLEGGSNOTAT
Møtesaksnr.: O-sak 2
Møtedato: 5. mai 2020
Notatdato: 8. april 2020
Arkivsaksnr.:
Saksbehandler: Bore, Grøndahl, Nenseth

TIL
UNIVERSITETSSTYRET

# Status på arbeidet med informasjonssikkerhet og personvern ved Universitetet i Oslo

I timene før regjeringen gikk ut med beskjeden om at barnehager, skoler og utdanningsinstitusjoner stenges, hadde alle IT-ansatte ved UiO et digitalt fellesmøte for å vurdere verktøy og kapasitet for videomøter og digital undervisning. Nye servere ble satt opp og kapasiteten skulle økes. I tillegg framskyndet USIT full bruk av nye digitale tjenester for videomøter, videoforelesninger og opptak. Selve lokalene ble stengt, men UiOs virksomhet skulle fortsette fra tusenvis av hjemmekontor, og all undervisning skulle over på digitale flater. I første omgang til over påske, samtidig ble det raskt tydelig at 12. mars 2020 innledet en ny digital hverdag på UiO og i samfunnet for øvrig. En hverdag som vil være med oss også den dagen studenter og ansatte igjen fyller campus.

I det følgende legger vi beskrivelsene i statusen fra 7. mai 2019 til grunn[1], og kommenterer endringer som er skjedd siden da. Som beskrevet i forrige status har UiO siden innføringen av EUs personvernforordning (GDPR) i 2018 hatt et særlig fokus på informasjonsarbeid og rutiner knyttet til etterlevelse av dette regelverket. Spørsmål rundt GDPR vil det også bli kommet tilbake til i forbindelse med en styresak om forskningsetikk.

## Digitalisering

Digitalisering i høyere utdanning og forskning er et kjerneområde i føringer fra Kunnskapsdepartementet (KD) og andre offentlige myndigheter. Digitalisering medfører at universitetets oppgaver kan effektiviseres og, som vi virkelig har sett de siste månedene, opprettholdes og videreutvikles selv om de fysiske lokalene stenges. Vi ser at arbeidsprosesser, undervisning og formidling utføres på effektive, nyskapende og kreative måter. Samtidig medfører digitalisering at stadig mer av universitetets verdier og beskyttelsesverdige informasjon behandles i komplekse tekniske løsninger, ofte hos tredjeparter og på ulike enheter. KDs digitaliseringsstrategi slår fast at det er behov for en målrettet styrking av arbeidet med informasjonssikkerhet og personvern. Vi ser nå mer enn noen gang at dette arbeidet er helt sentralt for å møte utfordringer som aktualiseres med nye IT-løsninger, slik at fremragende forskning og undervisning kan fortsette sikkert og uavbrutt – også fra kjøkkenbenken.

Den spesielle situasjonen vi internasjonalt nå er inne i, med COVID-19 og alt det innebærer, har ført til en eksplosjon i digitalisering, spesielt av undervisning. UiO har på veldig kort tid tatt grep

[1] O-SAK 3 Orientering om status for arbeidet med informasjonssikkerhet og personvern ved universitetet i Oslo

og flyttet fysisk undervisning til digital undervisning, og UiO har gjennomført i verdensklasse. Informasjonssikkerhetsaspektet er fulgt opp grundig gjennom hele prosessen; Risiko- og sårbarhetsanalyser har blitt gjennomført, og grunnsikring av tjenestene er tett fulgt opp. Nye IT-avtaler er gjennomgått og personvernet i tjenestene er vurdert og videreformidlet til sluttbrukerne. Vi har bygget opp en god kultur for å gjøre disse tingene riktig i mange år, og vi ser nå i en krisesituasjon at vi klarer å gjøre det også når det «brenner» rundt oss. I stedet for at personverneregelverket oppleves som en hindring for rask digitalisering, sikrer gode rutiner over flere år at digital undervisning og forskning kan komme opp nærmest over natta uten at det går på bekostning av personvernet eller informasjonssikkerheten i tjenestene.

En digitalisering som dette hadde ikke vært mulig uten kompetansen USIT og IT-virksomheten sitter på. Ved å klare å holde på et godt fagmiljø på tvers av informasjonsteknologien har organisasjonen vært i stand til å sammen snu seg rundt og virkelig levere. Dette hadde ikke vært mulig hvis UiO istedenfor å satse på USIT hadde satt ut leveranser til tredjepart.

I løpet av mars ble det arrangert 28.000 møter i Zoom, UiO sin nye plattform for videomøter/digital undervisning, med summert til sammen 227.000 deltakere. Klarere eksempel på at man har fått på plass noe som fungerer for ansatte og studenter er det vanskelig å se for seg. Karrieresenteret opplevde at en upassende innhold ble spredd i et stort åpent møte i midten av april. Vi mener at informasjonssikkerheten i Zoom er god, men ser at det kan være utfordringer med store åpne arrangement. Det arbeides kontinuerlig med dokumentasjon og informasjon rundt de ulike innstillingene man kan sette i Zoom for å minske sannsynligheten for tilsvarende episoder.

**Policy for informasjonssikkerhet**

Som ledd i at KD i fjor innførte en ny styringsmodell for informasjonssikkerhet, har Unit utarbeidet en policy for informasjonssikkerhet og personvern i høyere utdanning og forskning. Denne skal vedtas av KD og oppsummerer nasjonale føringer og lovkrav til informasjonssikkerhet og personvern. Policyen vil også være utgangspunktet for Units årlige kartlegginger av arbeidet med informasjonssikkerhet og personvern hos virksomhetene i sektoren.

I forslaget til policyen pekes det på viktigheten av at institusjonene har oversikt over eksportkontrollregelverket. Den siste tiden har også media hatt fokus på universitets- og høyskolesektorens etterlevelse av dette regelverket. Eksportkontroll innebærer at visse varer, teknologi og tjenester ikke kan eksporteres fra Norge uten lisens utstedt av Utenriksdepartementet. Særlig relevant for UiO er at immateriell teknologi og kunnskapsoverføring er dekket av regelverket. Internkontrollen for 2019 viser at det er et strukturelt problem at mange enheter mener at regelverket ikke er relevant. Regelverket er ikke nytt, men det har tidligere hatt noe begrenset fokus innad i sektoren. Det gjøres allerede arbeid på feltet, det er viktig at dette arbeidet fortsetter og at det sikres god kommunikasjon med Unit og KD. Utfordringene er felles for alle i sektoren, og det bør komme felles retningslinjer. Utenriksdepartementet utarbeider nå oppdaterte retningslinjer om eksportkontrollregelverket som er bedre tilpasset UH-sektoren, det er viktig at dette arbeidet følges opp på UiO, så vi sikrer at ansatte ved UiO ikke står i fare for å bryte regelverket.

**Ledelsessystem for informasjonssikkerhet**

I revisjonsrapporten «IT-beredskap – kontinuitetsplan», utført av Enhet for intern revisjon (EIR), ble det påpekt mangler i beredskaps- og kontinuitetsplaner. På bakgrunn av dette ble det våren 2019 utarbeidet ny beredskapsplan for USIT. Arbeidet ble utført med hjelp fra eksterne konsulenter. Planverket var ferdig sommeren 2019, og er nå tatt inn som en del av Ledelsessystem for informasjonssikkerhet (LSIS).

16. oktober 2019 gjennomførte USIT en IT-beredskapsøvelse. Dette var første øvelse etter nytt planverk. Øvelsen var utformet slik at situasjonen eskalerte til en større IKT-hendelse, som senere dannet grunnlaget for øvelse av sentral beredskapsledelse 18. oktober. Evalueringene som ble gjort i etterkant av begge øvelsene var svært positive.
Nytt planverk og øvelse har vist seg å være svært nyttig for effektivt kunne håndtere COVID-19-situasjonen.

LSIS skal gjennom en årlig ledelsens gjennomgang. Det har i løpet av 2019 ikke vært meldt inn eller avdekket behov for større endringer. Nytt beredskapsplanverk er tatt inn i LSIS og beskrivelse av internkontrollen er oppdatert for å reflektere dagens praksis.
Den delen av LSIS som er mest relevant for brukere flest er klassifiseringen av informasjonsressurser og lagringsguiden. Dette er veiledere om hvordan informasjonsressurser skal klassifiseres i en av de fire klassene - grønn, gul, rød eller svart. Lagringsguiden veileder brukerne om hvilke tekniske løsninger som er godkjent for hvilken klasse. Vi ser at dette klassifiseringssystemet har satt seg, og er godt implementert i organisasjonen, men det er et sterkt og økende behov for rådgiving og veiledning. Det jobbes kontinuerlig med å forbedre dokumentasjon og fagspesifikke veiledere for å sikre at informasjonsressurser klassifiseres likt og riktig på tvers av organisasjonen.

**Personvern i forskning**
Sist pekte vi på utfordringer knyttet til UiOs behov for å vurdere og godkjenne personvernet i forskningsprosjekter. Siden da har det foreslåtte tiltaket blitt gjennomført, og Norsk senter for forskningsdata (NSD) bistår nå UiO med å sikre og påvise at all behandling av personopplysninger til forskningsformål skjer i samsvar med personvernregelverket. Nye rutiner for forskning med personopplysninger er publisert på UiOs nettsider og Kvalitetssystemet for medisinsk og helsefaglig forskning er oppdatert i tråd med de nye rutinene. Videre er UiOs oversikt over forskningsprosjekter (Forskpro) utvidet til å kunne omfatte alle forskningsprosjekter ved UiO. Vi har gode erfaringer med denne prosessen som sikrer at personvernet blir ivaretatt på en trygg måte i forskningsprosjektene.

**Internkontroll**
Universitetet er pålagt å gjennomføre organisatoriske tiltak for å sikre overholdelse av personvernregelverket. Internkontrollen er et ledd i oppfyllelsen av denne forpliktelsen, og er inntatt i LSIS kapittel 14. Den årlige internkontrollen av behandlinger av personopplysninger ble gjennomført ved at ledelsen ved hver grunnenhet besvarte et nettskjema. 76,5 % av respondentene sier at de i stor grad har oversikt over alle behandlinger av personopplysninger ved enheten. Dette er en nedgang på 8 prosentpoeng fra i fjor.

På den annen side ble det ved forrige ledelsens gjennomgang pekt på et stort behov for videre opplæring i informasjonssikkerhet og personvern. Undersøkelsen fra internkontrollen viser at det er 70,6 % som i stor grad har fått informasjon om, eller opplæring i, hvordan disse opplysningene behandles. Dette er en oppgang på 8 prosentpoeng fra i fjor. Disse resultatene sett i sammenheng kan tyde på at når kunnskapsnivået om personvern går opp på enhetene, oppdager man at det er et komplisert område å ha fullstendig kontroll over. Det er likevel positive resultater, som viser at UiO har relativt god kontroll på behandling av personopplysninger.

På oppdrag fra UV-fakultetet utvikler LINK i samarbeid med juristene i IT-direktørens stab et e-læringskurs i personvern til forskere og studenter. Vi så også at når all undervisning ble digital oppstod det et stort behov for opplæring og veiledning i sikker bruk av digitale plattformer. Det ble lagt mye arbeid i å raskt produsere informasjonsinnhold og rutiner for ny digital bruk og å avklare sikkerhetsspørsmål i de nye tjenestene. Store deler av dette arbeidet er delt videre i sektoren.

**Trusselbildet**

UiO opplever trusselbildet som nokså uendret, det er jevnt økende med økende digitalisering. UiO har en robust infrastruktur som er godt rustet til å motstå økende trusler, men det kreves kontinuerlig vedlikehold.

PST påpeker i sin «Nasjonal trusselvurdering 2020» at «[u]*tenlandske etterretningstjenester forventes i 2020 å rette sin spionasje mot politiske myndigheter, mot naturressurser og næringsliv, mot forsvar og beredskap, samt mot forskning og utvikling*.» Etterretningstjenesten peker på det samme i «FOKUS 2020», og utdyper med «[f]*lere land benytter universiteter og forskningsinstitusjoner systematisk, og i stor skala, for anskaffelser til program for masseødeleggelsesvåpen og andre militære program*.» Dette tilsier at vi må, som tidligere nevnt, fortsette kartlegging og arbeid med etterlevelse av regelverk for eksportkontroll. Etterretningstjenesten påpeker at forskningssamarbeid vil utfordre eksportkontroll. UiO må, som resten av sektoren, finne en god balanse mellom kontroll og åpenhet.

Flere institusjoner har etterlyst klarere føringer fra myndighetene innenfor dette området.
Samlet sett viser trusselbildet oss fremdeles at det er et stort og voksende behov for ytterligere satsing på å bygge informasjonssikkerhetsmessig kompetanse, verktøy, ressurser og beredskap.

**Hendelseshåndtering og uønskede hendelser**

Det jobbes fremdeles målrettet med hendelseshåndtering ved UiO. Brudd på personopplysningssikkerheten og informasjonssikkerhetshendelser blir håndtert av UiOs eget hendelsesresponsteam, UiO-CERT, sammen med juristene i IT-direktørens stab. UiO-CERT samarbeider tett med andre hendelsesresponsteam, både nasjonalt og internasjonalt. I løpet av 2020 vil nøkkelpersoner fra UiO-CERT delta direkte inn i Uninett CERT og bidra direkte til hendelseshåndtering nasjonalt og på tvers i sektoren.

UiO-CERT håndterte i overkant av 2000 innkommende saker i 2019. Dette er en liten nedgang fra 2018, men samlet omfang i arbeid ligger på samme nivå. Håndtering av saker i et slikt omfang er mulig på grunn av veletablerte rutiner og høy kompetanse. Det er svært viktig at UiO klarer å opprettholde og videreutvikle kompetansen som er bygget opp gjennom mange år.
Nytt i 2019 er flere typer saker med forsøk på økonomisk svindel og utpressing, problemstillingen går igjen nasjonalt. Det er ikke kjent at UiO har lidd økonomiske tap på bakgrunn av dette, men det finnes enkeltepisoder hvor ansatte har blitt svindlet.

Vi ser en betydelig oppgang i innmeldinger av personsikkerhetsbrudd ved UiO, fra 17 i 2018 til 38 i 2019. Vi har grunn til å tro at dette skyldes at avviksrutinene stadig blir mer kjent i organisasjonen. Manglende tilgangsstyring og feilsendt informasjon er avvik som går igjen, og vi ser fremdeles et behov for grunnleggende opplæring i informasjonssikkerhet. Siden forrige gjennomgang har UiO meldt ett avvik til Datatilsynet. En melding i Canvas som innehold sensitive opplysninger om en student ble ved en feil sendt til alle deltagere på et emne. Datatilsynet og den berørte studenten ble raskt informert om hendelsen og hvilke tiltak som var iverksatt av UiO-CERT for å redusere personvernkonsekvensene.

**Videre arbeid**

UiO har arbeidet målrettet med informasjonssikkerhet og personvern i mange år gjennom etablering av ledelsessystem for informasjonssikkerhet, rutiner for sikker håndtering av personopplysninger og håndtering av avvik. I en situasjon der studenter må ta i bruk nye digitale tjenester for å kunne gjennomføre studiene, ser vi at både studenter og ansatte stiller krav til at personvernet og informasjonssikkerheten i tjenestene er ivaretatt. UiOs målrettede arbeid over flere år sikrer at alle IT-tjenester som blir godkjent for bruk ved UiO er grundig vurdert med

hensyn til informasjonssikkerhet, også i en tid der nye tjenester må tas i bruk tidligere enn forutsett.

Den teknologiske utviklingen går fort, og det er viktig at UiOs styre og toppledelse har fokus på informasjonssikkerhet og personvern i tiden som kommer.

Tilgang til høy kompetanse på det IT-sikkerhetsmessige og det IT-juridiske området er en forutsetning for både å kunne gi brukerne IT-løsninger som er innenfor rammene lov- og regelverk setter, og for å kunne håndtere avvik som måtte oppstå, raskt og mest mulig skadebegrensende. Vi ser at dette har vært særlig viktig de siste månedene, og dette blir stadig viktigere etter hvert som mer av IT-bruken på universitetet flytter ut fra universitetets maskinrom og ut i skybaserte tjenester, uavhengig av om disse befinner seg i private eller allment tilgjengelige skytjenester.

Trykket på informasjonssikkerhet og personvern er sterkt i dag og forventes å bli sterkere i årene som kommer. Dette innebærer at universitetet må vie det mer oppmerksomhet og prioritere ressurser for blant annet:

- Å sette informasjonssikkerhetsorganisasjonen nedfelt i LSIS bedre i stand til å følge opp sitt ansvar og sine oppgaver kompetanse-, verktøy- og rutinemessig
- Å styrke det operative informasjonssikkerhetsarbeidet i IT-organisasjonen (sentralt og lokalt)
- Å øke brukenes bevissthet om truslene og hvordan de best kan beskytte seg og arbeide med minst mulig risiko for å bryte informasjonssikkerheten

I de senere årene har det skjedd en endring i vårt sikkerhetsarbeid. Der det tidligere ble jobbet reaktivt og man håndterte en hendelse i det den ble oppdaget, jobbes det nå proaktivt, man leter aktivt etter hendelser i store mengder loggdata. UiO-CERT har for å holde seg helt i forkant i dette arbeidet, inngått samarbeid med forskningsmiljøet ved Institutt for informatikk som har informasjonssikkerhet som fagfelt, og ønsker å styrke dette arbeidet fremover. Bakgrunnen for at det er mulig å arbeide proaktivt er beskrevet i detalj i forrige orientering til styret (7. mai 2o19) og skyldes i korte trekk at det har vært gjort grundig arbeid med grunnsikring, samt en god og stabil drift i mange år.

Tradisjonelt har uønskede personvern- og IT-sikkerhetshendelser vært noe mange ikke har ønsket å snakke om offentlig. UiO har hatt lang tradisjon for åpenhet rundt slike hendelser. Hemmelighold holder fagfeltet tilbake, det er ved å være åpne og ærlige at vi sammen kan lære hvordan best håndtere cybertrusler. UiO bør fortsette med denne praksisen.

---

Vedlegg:

- Status informasjonssikkerhet
- Status personvern

| Krav | Tilstand 2019 | Tilstand 2020 | Status på eksisterende tiltak | Behov for tiltak |
|---|---|---|---|---|
| **Gjennomført/revidert ROS-analyse i 2017/2018** | | | | |
| ROS analyser på administrative systemer og på infrastruktur komponenter | God | God | Som en del av GDPR prosjektet i 2018 ble det gjennomført og/eller oppdatert ROS på alle kartlagte IT-systemer. Disse følges opp annenhvert år, eller ved større endringer. | |
| ROS analyse av USIT | Tilfredstillende | Tilfredstillende | Det er ikke gjennomført en egen ROS av USIT som driftsleverandør. Dette er planlagt i 2020 | |
| ROS av systemer i forskning og utdanning | Ikke tilfredstillende | Tilfredstillende | Et nytt nettskjema for egenrapportering av mindre skytjenester til bruk i forskning og utdanning bidrar nå til at flere systemer blir registrert og får gjennomført en nødvendig vurdering av personvern og informasjonssikkerhet. Det oppdages fremdeles flere systemer i bruk på UiO som ikke er godkjent, men oftere enn i fjor er dette systemer som brukes i mindre skala. | Det må etableres en prosess for å styre valg av verktøy og tjenester i bruk for forskning og utdanning. Det må sikres at tjenester som er tatt i bruk skjer lovlig, med de nødvendige avtaler på plass. |

| Krav | Tilstand 2019 | Tilstand 2020 | Status på eksisterende tiltak | Behov for tiltak |
|---|---|---|---|---|
| Gjennomført og evaluert en kriseøvelse i 2018 | | | | |
| Generell kriseøvelse | God | God | Gjennomført høsten 2018. | |
| Spesifikk øvelse på informasjonssikkerhet | Tilfredstillende | God | Gjennomført høsten 2019. Lokalt på USIT og sammen med sentral kriseledelse (SBL). | |
| Evaluering av kriseøvelse | Tilfredstillende | God | Gjennomført høsten 2019. | |
| | | | | |
| **Krav** | **Tilstand 2019** | **Tilstand 2020** | **Status på eksisterende tiltak** | **Behov for tiltak** |
| Ledelsessystem for informasjonssikkerhet - LSIS | | | | |
| Ledelsessystem for informasjonssikkerhet gjort kjent i organisasjonen | God | God | Ila. våren 2019 er det gjennomført en bred informasjonsrunde med bekjentgjøring av LSIS i hele organisasjonen. | Informasjonsrunden har avdekket at det er et kontinuerlig behov for opplæring og informasjon om temaet. Det jobbes med å få på plass e-læring. |
| Kartlegging av kjennskap og etterlevelse av LSIS | God | God | Som en del av internkontrollen er det vinteren 2020 gjennomført en kartlegging av kjennskap til, og etterlevelse av gjeldene regelverk for informasjonssikkerhet og personvern | |

| Krav | Tilstand 2019 | Tilstand 2020 | Status på eksisterende tiltak | Behov for tiltak |
|---|---|---|---|---|
| Ledelsessystem for informasjonssikkerhet - LSIS | | | | |
| Oppfølging av funn i kartleggingen | Tilfredstillende | Tilfredstillende | Kartleggingen viser tildels store mangler i kjennskap og etterlevelse ved enkelte enheter | Målrettede tiltak mot enkelte enheter. |
| Ledelsens gjennomgang | Tilfredstillende | God | Gjennomført som årlig rapportering til Universitetsstyret | |
| Grunnsikring - KD oppfordrer institusjonene til å løfte informasjonssikkerheten høyere enn de nasjonale minstekravene. | God | God | UiO har i LSIS videreført krav om grunnsikring. UiO har lange tradisjoner for felles drift, oppsett og konfigurasjon av systemer. Med noen lokale tilpassinger er alle tiltak i NSMs «ti viktige tiltak mot dataangrep» iverksatt på UiO. | Vurdere om en skal innvilge færre unntak fra sikringen, og stramme inn. |
| Internkontroll på informasjonssikkerhetsområdet | God | God | Gjennomført sammen med internkontroll for bruk av personopplysninger våren 2019 og igjen våre 2020. | |
| | | | | |

| Krav | Tilstand 2019 | Tilstand 2020 | Status på eksisterende tiltak | Behov for tiltak |
|---|---|---|---|---|
| Hendelseshåndtering | | | | |
| Har institusjonen innført rutine for å håndtere uønskede digital hendelser | God | God | UiO-CERT er UiOs operative hendelsesteam. De har eksistert siden 2005, har gode og dokumenterte rutiner med god nasjonalt og internasjonalt nettverk. | |
| IT-beredskap og kontinuitetsplan | Tilfredstillende | Tilfredstillende | Ny IT-beredskapsplan er innført, trent og øvd. Det er mangler ved kontinuitetsplaner | Det må innføres konfinuitetsplaner for viktige prosesser. Dette må følges opp også utenfor USIT. |
| | | | | |
| **Krav** | **Tilstand 2019** | **Tilstand 2020** | **Status på eksisterende tiltak** | **Behov for tiltak** |
| Eksportkontroll | | | | |
| Har institusjonen oversikt over kunnskapsområder som reguleres av eksportkontroll-lovgivningen | | Ikke tilfredstillende | Interkontrollen 2019 viser at enhetene ikke har god nok oversikt over eksportkontroll-regelverket | UiO må innføre oppdaterte retningslinjer når dette foreligger fra UD |
| Etterlever institusjonen eksportkontroll-lovgivningen | | Ikke tilfredstillende | Interkontrollen 2019 viser at enhetene ikke har god nok etterlevelse av eksportkontroll-regelverket | UiO må kartlegge hva som er underlagt regelverket og gjøre nødvendige tiltak |

| Krav | Tilstand 2019 | Tilstand 2020 | Status på eksisterende tiltak | Behov for tiltak |
|---|---|---|---|---|
| **Krav om oversikt over all behandling av personopplysninger i forskning** | | | | |
| *Medisinsk og helsefaglig forskning* | Tilfredstillende | God | Oversikt over medisinsk- og helsefaglige forskningprosjekter (tidligere Helseforsk) ble i 2019 utvidet til å kunne registrere alle forskningsprosjekter ved UiO og skiftet navn til Forskpro. | Våren 2020 arbeides det med å utvikle en integrasjon mellom Forskpro og NSD slik at forskningsprosjekter automatisk hentes fra NSD-portalen og forsker unngår dobbeltregistrering. |
| *Forskning på øvrige personopplysninger* | God | God | NSDs meldingsarkiv gir en oversikt over UiOs forskning på personopplysninger. Alt som skal til NSD meldes i stor grad til NSD. | |

| | | | | |
|---|---|---|---|---|
| **Krav om oversikt over all behandling av personopplysninger** | | | | |

| | | | | |
|---|---|---|---|---|
| *Register over administrative behandlinger* | Tilfredstillende | Tilfredstillende | Oversikt over administrative behandlinger av personopplysninger (meldeappen) er oppdatert i 2020 for å gjøre den mer brukervennelig. Det er fremdeles mangelfulle registreringer. | Kreves større bevissthet og bedre kontroll fra ledelsen på enhetene om lovlig bruk av systemer og større bevissthet rundt hvilke systemer og behandlinger som skal registreres i meldeappen. Det arbeides med en veiledning for hva som skal registreres for å sikre etterlevelse. |
| *Oversikt over systemer brukt i forskning og utdanning* | Ikke tilfredstillende | Tilfredstillende | Et nytt nettskjema for egenrapportering av mindre skytjenester til bruk i forskning og utdanning bidrar nå til at flere systemer blir registrert og får gjennomført en nødvendig vurdering av personvern og informasjonssikkerhet. Det oppdages fremdeles flere systemer i bruk på UiO som ikke er godkjent, men oftere enn i fjor er dette systemer som brukes i mindre skala. | Det må fremdeles kommuniseres tydelig fra enhetene at man kun kan ta i bruk systemer som UiO har godkjent slik at UiO har kontroll på informasjonssikkerheten og personvernet. Nettskjemaet for egenrapportering av mindre tjenester må bli bedre kjent på enhetene. |

| | | | | |
|---|---|---|---|---|
| **Krav om intern forankring/godkjennelse av alle forskningsprosjekt som behandler personopplysninger** | | | | |

| | | | | |
|---|---|---|---|---|
| *Medisinsk- og helsefaglige forskningsprosjekter* | Tilfredstillende | God | Fjorårets foreslåtte tiltak er gjennomført og tjenesteavtalen med NSD om vurderinging av forskningsporsjekter som behandler personopplysninger, er nå utvidet til også å omfatte medisinske og helsefaglige prosjekter. NSD bistår forsker med personvernkonsekvensvurdering (DPIA) når dette er nødvendig. | |
| *Forskning på øvrige personopplysninger* | God | God | Tjenesteavtale med NSD om gjennomgang og godkjennelse av forskning på personopplysninger. | |

| **Krav om internkontroll** | | | | |
|---|---|---|---|---|
| *Generelle veiledere* | God | God | Oppdaterte generelle rutiner og veiledere for behandling av personopplysninger i forskning og i administrasjonen. | |
| *Internkontroll/Kvalitetssystem for forskning på personopplysninger* | Tilfredstillende | Tilfredstillende | Rutine for forskning med personopplysninger er vedtatt og publisert. Kvalitetssystemet for medisinsk og helsefaglig forskning er oppdatert for å speile de nye rutinene om søknad til NSD for all forskning med personopplysninger. | Rutinene for forskning på personopplysninger skal utvides til å tydeligere avklare roller og ansvar på UiO ved behandling av personopplysninger i forskning. |

| | | | | |
|---|---|---|---|---|
| *Dedikerte personer på enhetsnivå med ansvar for personvern* | God | God | Personvernkontakter på alle enheter blir kurset til å kunne besvare personvernspørsmål fra egen enhet. Bidrar til kompetanseheving og oversikt over personverrettslige problemstillinger og løsninger på egen enhet. | |
| *Kursing og veiledning av ansatte/forskere/studenter* | Tilfredstillende | Tilfredstillende | Opplæringsprogram på UiOs enheter ved behov og på forespørsel. Utøver av behandleransvaret holder 1-2 kurs/presentasjoner i uken for studenter og ansatte på alle enheter. Spørsmål om personvern besvares fortløpende på telefon og e-post. Personvernkontakter kurses slik at de kan besvare spørsmål fra egen enhet. | E-opplæring for universitetets studenter og forskere planlegges utrullet våren 2020, i første omgang ved UV-fakultetet. |
| *Internkontrollsystem* | God | God | Internkontrollsystem i form av årlig skriftlig interkontroll/brevkontroll og stedlig kontroll er revidert og implementert. Ledere ved alle enheter besvarte en skriftlig internkontroll i mars 2019 og stedlige kontroller gjennomføres fortløpende med spesifikke tema i fokus. | |
| | | | | |
| **Krav om ett overordnet personvernombud** | God | God | Konstituert personvernombud er ansatt i 100% stilling. Stillingsinstruks er vedtatt av Universitetsstyret. | |