UNIVERSITETET
I OSLO

Notat

Til:
LOS UiO:Ledelsen og støtteenheter

Dato: 22.04.2022
Saksnr..: 2022/10360 VILDESN

Unntatt offentlighet: offl § 14

Resultat av internkontroll av behandling av personopplysninger for 2021

Universitetet i Oslo er pålagt å ha organisatoriske tiltak for å sikre overholdelse av personvernregelverket. Internkontrollen er et ledd i oppfyllelsen av denne forpliktelsen og er inntatt i Ledelsessystem for informasjonssikkerhet (LSIS) kapittel 14.

Den årlige internkontrollen av behandlinger av personopplysninger ved universitetet har siden 2019 blitt gjennomført ved at ledere ved hver grunnenhet besvarer et spørreskjema. I forkant av årets undersøkelse ble fakultetsdirektører, instituttledere, senterledere, avdelingsdirektører og andre aktuelle enhetsledere varslet om internkontrollen. De inviterte mottok en personlig lenke til undersøkelsen i Nettskjema på e-post, samt påminnelser hver uke mens undersøkelsen var åpen dersom de ikke hadde svart. Undersøkelsen var i første omgang åpen i tre uker fra 24.01.22. På grunn av manglende svar fra noen av respondentene var undersøkelsen åpen til 23.02.22.

I den årlige internkontrollen for 2021 ble det sendt 68 invitasjoner og levert 64 svar. Internkontrollen ble sendt til både administrative og vitenskapelige ledere. I det følgende vil vi gjennomgå de viktigste resultatene fra undersøkelsen.

Oversikt og opplæring
75 % av respondentene sier at de i stor grad har oversikt over alle behandlinger av personopplysninger ved enheten. Dette er en liten nedgang fra i fjor. Videre melder 65,6 % at det i stor grad er gitt informasjon om, eller opplæring i, hvordan disse opplysningene behandles. Dette er en nedgang på 12,3 prosentpoeng fra i fjor. Dette viser at kunnskapen om behandling av personopplysninger på et overordnet nivå har redusert noe i 2021, etter flere år med økning. Likevel må UiO sies å ha relativt god kontroll på behandlingen av personopplysninger. Resultatene fra de mer detaljerte spørsmålene viser imidlertid at innenfor visse områder er det fortsatt begrenset kjennskap til en del av UiOs rutiner og gjeldende lovkrav.

I årets internkontroll melder omlag 10% at enhetene i liten grad har nok ressurser til å følge opp personvernregelverket, men ingen melder at de ikke i det hele tatt har nok ressurser. Dette er en liten, men positiv nedgang fra i fjor. Det er i år, som tidligere år, primært forskningsenhetene som melder at de har for lite ressurser til å følge opp personvernregelverket. Heller ikke i år er det noen fakulteter som skiller seg ut hva gjelder ressurssituasjonen. Nytt i år er at det ble inkludert et fritekstfelt i undersøkelsen, og flere respondenter ytret et behov for, og ønske om, mer opplæring ved enhetene.

UiO:Ledelsen og støtteenheter
Universitetets senter for informasjonsteknologi
Stabsfunksjoner og interne støttetjenester

Postadresse:
Postboks 1059 Blindern
0316 OSLO

Besøksadresse:
Kristen Nygaards hus,
Gaustadalléen 23 A, 0373
Oslo

Tlf: 22 85 24 70
Faks: 22 85 27 30
E-post: postmottak@usit.uio.no
www.usit.uio.no
Org.nr.: 971 035 854

Personopplysninger i forskning
Internkontrollen viser at det er en økning i kjennskapen til rutiner for å melde forskningsprosjekter til Sikt (tidligere Norsk senter for forskningsdata (NSD)). I år er det over 70% av respondentene fra vitenskapelig linje som svarer at enheten deres har gode rutiner for å melde prosjekter til Sikt for en vurdering av personvernet. Kun 3% melder de i liten grad har kjennskap til rutiner for dette. Videre er det positivt at det er en markant nedgang i antall enheter innen vitenskapelig linje som melder at det ikke er relevant å ha rutiner for å melde forskningsprosjekter til Sikt.
Når det kommer til medisinsk- og helsefaglig forskning viser internkontrollen at over halvparten av respondentene i vitenskapelig linje i stor grad har kjennskap til rutiner for å melde forskningsprosjekter til Regionale etiske komiteer (REK), mens for 35,3% er det ikke relevant.

Hva gjelder informasjon til forskere om hvordan personopplysninger i forskningsprosjekter skal behandles, viser resultatene at det er en oppgang innen vitenskapelig linje fra fjorårets internkontroll. Det er over 75% som svarer at forskere i stor grad har fått informasjon om hvordan personopplysninger i forskningsprosjekter skal behandles, hvilket er en økning på 14 prosentpoeng fra fjoråret. 6% av respondentene svarer at forskere som behandler personopplysninger i liten grad har fått informasjon om hvordan personopplysningene skal behandles. Det er videre 11,8 % som svarer at det ikke er relevant å gi forskere denne informasjonen, hvilket er en liten nedgang fra fjorårets interkontroll. Utøver av behandleransvaret vil gå i dialog med de som har svart at det ikke er relevant å ha rutiner for behandling av personopplysninger i forskningsprosjekter, for å undersøke hvorfor dette er svart.

Meldeappen
Interkontrollen viser at det fortsatt er noe begrenset kunnskap om registrering i UiOs oversikt over administrative behandlinger av personopplysninger («meldeappen»). Resultatene viser at 12,5 % har systemer/behandlinger som skulle vært registrert, men som ikke er det. Dette er omtrent det samme resultatet som tidligere år. Resultatene viser også at det er 31,1 % som ikke vet om de har systemer som skulle vært registret. Dette er en økning fra fjorårets resultat. 3,1% vet ikke om enheten følger rutiner for at alle systemer som skal registreres i meldeappen faktisk registreres, og 6,3% mener det ikke er relevant. Resultatene tyder på et behov for mer kunnskap om meldeappen.

Ledelsessystemet for informasjonssikkerhet
Ledelsessystemet for informasjonssikkerhet (LSIS) er et sett med dokumenter som beskriver og angir hvordan arbeidet med informasjonssikkerhet ved UiO skal foregå. For å sikre at dette arbeidet forvaltes riktig, er det viktig at alle som arbeider og studerer ved UiO er kjent med hvordan informasjonssikkerheten ved universitetet skal ivaretas.
Enhetenes kjennskap til LSIS er tilnærmet lik resultatet fra de to foregående årene. Selv om kjennskapen ikke har blitt redusert, anser utøver av behandlingsansvaret at kunnskapen om LSIS fortsatt for lav ved enhetene. Det er kun 26,6 % som melder fra om at LSIS i stor grad er kjent ved deres enhet, og 42,2 % melder om at det er i moderat grad kjent. Det er 23,4% som melder at LSIS er i liten grad kjent, og nesten 5% kjenner ikke til LSIS i det hele tatt. Resultatene viser at kunnskapen om LSIS er for lav ved UiO, og det bør prioriteres fra USIT at kunnskapen om ledelsessystemet blir bedre i institusjonen, eksempelvis ved å gjenoppta informasjonskampanjer om LSIS lik de som ble utført i 2019.

Til tross for at kjennskapen til LSIS fortsatt er begrenset, viser internkontrollen at rutinene som følger av LSIS i ganske stor grad blir fulgt og er kjent ved UiO. Rett over halvparten melder at LSIS etterleves i stor grad, 30% i moderat grad, mens omkring 15% vet ikke hvorvidt LSIS etterleves.

Det er 6,3 % som melder fra om at enheten i liten grad kjenner til retningslinjer for klassifisering av data og informasjon. Det er også bare 6,3 % som melder at de ikke vet om retningslinjene er kjent ved deres enhet. Dette er en liten negativ utvikling fra i fjor, men resultatet er fremdeles positivt og viser at UiOs lagrings- og klassifiseringsguide er godt kjent ved enhetene. Dette viser at UiO har forholdsvis god kontroll på dataene vi forvalter, men det er fortsatt store muligheter for forbedring.

De innleverte svarene viser at enhetene generelt har gode rutiner for vedlikehold av tilgangen til IT-systemer. 78,1 % melder at de i stor grad har rutiner for vedlikehold av tilganger til systemer – en økning på 7,5 prosentpoeng fra i fjor. I 75 % av tilfellene etterleves disse rutinene i stor grad, og 10,9% i moderat grad. 12,5% melder det ikke er relevant med verken rutiner for vedlikehold av tilgang til IT-systemer eller etterlevelse.

Avvikshåndtering
Årets resultater viser at henholdsvis 10,9 % av de ansatte ved enheten i liten grad kjenner til rutiner for håndtering av avvik ved personopplysnings- og 6,3 % kjenner i liten grad til rutiner for håndtering av informasjonssikkerhetshendelser. Dette er mer enn en halvering fra fjorårets undersøkelse av hvor mange som i liten grad kjenner til UiOs avvikshåndteringsrutiner, og andelen som i moderat eller stor grad kjenner til rutinene øker. Dette er å anse som en positiv utvikling. *Ingen* melder at de ansatte ikke kjenner til rutinene for håndtering av avvik ved behandling av personopplysninger, og bare 1,6 % melder at de ansatte ved enheten ikke kjenner til UiOs rutiner for håndtering av informasjonssikkerhetshendelser. 73,4 % har svart at ledelsen i stor grad kjenner til rutiner for håndtering av avvik ved behandling av personopplysninger og 65,6 % for informasjonssikkerhetshendelser. Dette er en stor positiv økning fra fjoråret.
Dette resultatet gjenspeiles også i at antall innmeldte avvik fra enhetene i 2021 har økt betydelig, fra 24 innmeldte avvik i 2020 til 40 innmeldte avvik i 2021. Vi har grunn til å tro at dette ikke skyldes at det skjer flere avvik ved håndtering av personopplysninger nå enn tidligere, men at rutinene for å melde de avvikene som skjer er bedre kjent ved enhetene. Det er likevel 17,2% av respondentene melder at de ikke vet om enheten har hatt avvik det siste året som ikke har blitt rapportert til UiO-CERT, noe som indikerer at opplæring i avviksrutiner fortsatt bør ha fokus fremover.

Eksportkontroll
I «Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning»[1] fremgår det at det er viktig at institusjonene har kontroll på eksportkontrollregelverket. I tillegg har også media de siste årene hatt fokus på etterlevelsen av dette regelverket i UH-sektoren. På bakgrunn av dette har det de siste to årene blitt stilt spørsmål om oversikt og etterlevelse av eksportkontrollregelverket. Eksportkontroll innebærer at visse varer, teknologi og tjenester ikke kan eksporteres fra Norge uten lisens utstedt av Utenriksdepartementet (UD).[2] Særlig relevant for UiO er at immateriell teknologi og kunnskapsoverføring er dekket av regelverket.[3] Regelverket er ikke nytt, men det har vært noe begrenset fokus innad i UH-sektoren på området. Dette gjenspeiles også i år i resultatene. Det er 20,3 % og 31,3 % som i henholdsvis moderat og stor grad har oversikt over regelverket på sine enheter. Dette er en totalt sett liten økning sammenlignet med fjorårets internkontroll. Det er videre 39,1% som mener at regelverket ikke er relevant, noe som er en liten reduksjon fra fjorårets resultat.

Når det kommer til etterlevelse mener over halvparten at regelverket ikke er relevant for deres enhet. Det er problematisk at så mange enheter mener at regelverket ikke er relevant – i år som i fjor, og kunnskapen om regelverket må økes ved UiO.

I april 2022 kom Utenriksdepartementet med et høringsforslag om endringer i eksportkontrollforskriften knyttet til en lisensordning for kunnskapsoverføring. Ifølge departementet er formålet med de foreslåtte reglene å sikre målrettet kontroll med at kunnskapsoverføring fra UH-sektoren foregår i tråd med norsk sikkerhets- og forsvarspolitikk. UiO bør innføre oppdaterte retningslinjer og rutiner for å sikre at ansatte ved UiO ikke står i fare for å bryte regelverket.

Særlig om hjemmekontor
På grunn av Covid-19 pandemien var det også i 2021 mange ansatte som jobbet fra andre steder enn kontoret. I fjorårets internkontroll ble det stilt spørsmål vedrørende hjemmekontor, som ble videreført i årets undersøkelse. Over halvparten av respondentene melder at hjemmekontor ikke har skapt utfordringer eller har skapt få utfordringer for etterlevelse av rutiner for personvern og informasjonssikkerhet. Det ble også stilt spørsmål ved om det har vært problemer for de ansatte å ha tilgang til godkjent utstyr og om det har vært mangler i IT-tjenestene til at de ansatte kunne utføre sine arbeidsoppgaver. 20,3% av respondentene hadde i moderat grad hatt problemer med å stille til rådighet godkjent utstyr. Dette var en reduksjon på 13,5 prosentpoeng fra året før. 4,7 % mente at det i stor grad var problemer med å stille godkjent utstyr til rådighet for ansatte på hjemmekontor. Hva gjelder mangler i IT-systemer, meldte 28,1% at det i moderat grad og 5,9 % at det i stor grad var mangler i IT-tjenestene til UiO. Det var en økning på 6 prosentpoeng fra i fjor på moderat grad, og en reduksjon på 4 prosentpoeng på stor grad av mangler ved IT-tjenestene. Resultatene viser at respondenter innen teknisk/administrativ linje i mindre grad har møtt utfordringer i forbindelse med hjemmekontor enn i vitenskapelig linje.
Tallene viser at UiO var teknisk jevnt over ganske godt rustet for hjemmekontor – og bedre rustet enn i fjor, men at det likevel har vært noen utfordringer. Nå som brorparten av de ansatte er tilbake på kontoret og eventuell bruk av hjemmekontor er godt etablert ved UiO, antar vi at færre vil rapportere om disse utfordringene i fremtiden.

Oppsummering
UiO har i mange år har jobbet systematisk med informasjonssikkerhet og personvern. Dette, sammen med det økte fokuset i media, har hatt en positiv innvirkning på kunnskapen om personvern og IT-sikkerhet, slik at det generelle nivået ved UiO fremdeles er relativt godt. Også årets internkontroll viser at enhetene i hovedsak har god oversikt over og i stor grad etterlever UiOs rutiner på området. Vi ser imidlertid at det på noen områder fortsatt finnes et klart forbedringspotensial, slik som ved opplæring av ansatte i gjeldende rutiner ved UiO, og da særlig om LSIS og avviksrutiner. Dette kan blant annet avhjelpes med UiOs nye e-læringskurs om personvern i Canvas som skal gi grunnleggende kunnskap om personvern, informasjonssikkerhet og UiOs rutiner. Fritekstfeltene i årets internkontroll avdekket også et ønske om mer kursing i personvern. Dette er noe vi vil fortsette å prioritere fremover. Dette er et arbeid som vi ser på som svært viktig for å sikre at oppmerksomheten rundt behandling av personopplysninger og informasjonssikkerhet opprettholdes og økes.

Foreslåtte tiltak utøver av behandlingsansvaret vil følge opp:

- Opplæring i UiOs rutiner for håndtering av avvik ved behandling av personopplysninger og informasjonssikkerhetshendelser, samt oppdatering og presisering av nettsidene på området
- Opplæring og informasjonskampanje om LSIS
- Promotering av det nye e-læringskurset om personvern og UiOs rutiner på området i Canvas for vitenskapelige ansatte
- Ferdigstille e-læringskurs for administrativt ansatte
- Opplæring i bruk av meldeappen
- Direkte kontakt og oppfølging av de enhetene som undersøkelsen viser har behov for veiledning på visse punkter

Vi tar også med oss tilbakemeldinger som ble gitt i fritekstfeltene når vi skal utforme og sende ut neste års internkontroll. Utøver av behandleransvaret er tilgjengelig via e-post: behandlingsansvarlig@uio.no.

Takk til alle som svarte på årets undersøkelse.

Med hilsen

Lars Oftedal
IT-direktør

Vilde Sørbø Nenseth
Utøver av behandleransvaret

Dette dokumentet er godkjent elektronisk ved UiO og er derfor ikke signert.

Kopi til:
Enhet for intern revisjon

Saksbehandler:
Vilde Sørbø Nenseth
v.s.nenseth@usit.uio.no