UiT Norges arktiske universitet

Årsrapport 2021

Personvernombud

Joakim Bakkevold

Innholdsfortegnelse

1. Personvernombudets rolle og oppgaver

1.1 Personvernombudets rolle

Personvernombudets rolle er fastsatt i personvernforordningen (GDPR) artikkel 38.

Personvernombudet har en uavhengig rolle i forhold til universitetet som behandlingsansvarlig ved behandling av personopplysninger. Personvernombudet kan ikke instrueres av behandlingsansvarlig og skal rapportere til universitetets ledelse.

Overordnet skal personvernombudet bidra til at universitetet ivaretar personvernet til ansatte, studenter, forskningsdeltakere og andre universitetet behandler personopplysninger om. De registrerte kan kontakte personvernombudet angående alle spørsmål om behandling av deres opplysninger og utøvelsen av deres personvernrettigheter ved universitetet. Personvernombudet har taushetsplikt etter personopplysningsloven § 18. Dette omfatter blant annet personlige forhold, sikkerhetstiltak og enkeltpersoners varsling om overtredelse av personvernregelverket.

UiT Norges arktiske universitet og Samisk høgskole har i 2021 hatt felles personvernombud.

1.2 Personvernombudets oppgaver

Personvernombudets oppgaver er fastsatt i personvernforordningen artikkel 39. I tillegg er oppgavene nærmere beskrevet i universitetets ledelsessystem for informasjonssikkerhet og personvern kapittel 3.

Personvernombudet skal informere og gi råd til universitetet og de som behandler personopplysninger på vegne av universitetet, om de forpliktelser de har etter personvernforordningen.

Personvernombudet skal kontrollere blant annet overholdelsen av personvernforordningen, universitetets egne personvernregler og universitets holdningsskapende tiltak og opplæring av behandlere.

Personvernombudet skal på anmodning gi råd om vurderingen av personvernkonsekvenser (DPIA) og kontrollere gjennomføringen av den.

Personvernombudet skal samarbeide med Datatilsynet og fungere som Datatilsynets kontaktpunkt ved spørsmål om behandlinger av personopplysninger ved universitetet.

Personvernombudet har ikke beslutningsmyndighet på vegne av den behandlingsansvarlige.

2. Involvering og kontaktpunkter internt

2.1 Involvering

Universitetet skal sikre at personvernombudet blir involvert på riktig måte og til rett tid i alle spørsmål som gjelder vern av personopplysninger.

Personvernombudet har i 2021 hatt regelmessige møter med universitetsledelsen ved assisterende universitetsdirektør Gøril Heitman. På grunn av endringer i ledelsen må det for 2022 avklares hvem som blir ny kontaktperson i ledelsen for personvernombudet.

Personvernombudet er fast deltaker i universitets informasjonssikkerhetsforum.

2.2 Kontaktpunkter internt

Avdeling for IT har en egen faggruppe for informasjonssikkerhet og personvern. Tilsatte i Avdeling for IT og Faggruppe for informasjonssikkerhet og personvern er naturlig kontaktpunkt for personvernombudet.

Videre er en tilsatt knyttet til ledelsen i Avdeling for forskning, utdanning og formidling kontaktpunkt for Norsk senter for forskningsdata (NSD), som ved avtale leverer personverntjenester til universitetet for forsknings- og studentprosjekter hvor det skal behandles personopplysninger. Denne kontaktpersonen og NSD er naturlige samarbeidspartnere for personvernombudet.

Det helsevitenskapelige fakultet har flest forsknings- og studentprosjekter hvor det behandles personopplysninger. Personvernombudet har fast kontaktperson ved fakultetets Seksjon for forskning, utdanning og formidling. Personvernombudet savner lignende kontaktpunkt ved Fakultet for humaniora, samfunnsvitenskap og lærerutdanning. Dette fakultetet har også mange forsknings- og studentprosjekter hvor det behandles personopplysninger.

Personvernombudet savnet et fast forum for tilsatte som arbeider med personvern på ulike enheter, som møtes regelmessig for å drøfte og ta stilling til personvernspørsmål og hvordan disse bør håndteres.

3. Mottak av saker

Universitetet opplyser om personvernombudets kontaktinformasjon og oppgaver på sine nettsider, https://uit.no/om/art?p_document_id=594059&dim=179007 Innholdet på siden forvaltes av personvernombudet. Personvernombudet kan nås per telefon og e-post, personvernombud@uit.no. De aller fleste henvendelsene til personvernombudet kommer fra tilsatte og studenter, som behandler eller skal behandle personopplysninger på vegne av UiT som behandlingsansvarlig. I hovedsak gjelder det forsknings- eller studentprosjekter, men også fra deler av administrasjonen.

I alle forsknings- og studentprosjekter skal det opplyses om personvernombudets kontaktinformasjon. De registrerte tar i liten grad kontakt med personvernombudet. Det kan tyde på at de registrerte

generelt har stor tillitt til behandlingen som utføres i prosjektet og har fått god informasjon om prosjektet de deltar i. Personvernombudet opplever det også slik at de registrerte tar kontakt direkte med prosjektets kontaktperson ved spørsmål og ønske om innsyn i sine opplysninger.

Videre tar både tilsatte og studenter kontakt angående ulike administrative behandlinger, som personvernombudet følger opp ovenfor de som ivaretar det daglige behandlingsansvaret. De tar disse henvendelsene fra personvernombudet på alvor, herunder de redegjør for hvilke rutiner som gjelder eller iverksetter nødvendige tiltak.

NSD kontakter også personvernombudet ved personvernspørsmål knyttet til universitetets prosjekter meldt til NSD.

4. Internkontroll ved universitetet

Personvernombudet skal etter personvernforordningen blant annet kontrollere universitetets overholdelse av personvernregelverket og tilhørende revisjoner.

Personvernombudet deltok 8.3.2021 i møte med Unit, nå HK-dir, og universitetsledelsen om status for arbeidet med informasjonssikkerhet og personvern ved universitetet. Statusen blir kartlagt ved at universitetet i møtet gir muntlige svar på spørsmål i et kartleggingsskjema. I etterkant av kartleggingen får universitetet fra Unit anbefalinger for det videre arbeidet med informasjonssikkerhet og personvern.

Universitetsstyret har bedt om at det gis en uavhengig vurdering, revisjon, av status innen informasjonssikkerhet og personvern, samt at det gis innspill til eventuelle forbedringsmuligheter og relevante tema for oppfølgingsrevisjoner.

PricewaterhouseCoopers AS (PwC) har på oppdrag fra universitetet i 2021 gjennomført revisjon innen informasjonssikkerhet og personvern, ut fra et internkontrollperspektiv.

Personvernombudet har vært involvert i revisjonen. Dette i innledende samtaler om gjennomføringen av revisjonen, som intervjuobjekt og i forbindelse med ferdigstillelsen av revisjonen.

Personvernombudets oppfatning er at internrevisjonsrapporten fra PwC gir et godt og riktig bilde av statusen for universitetets arbeid innen informasjonssikkerhet og personvernombud. PwC har gjennomført en rekke intervjuer med tilsatte på tvers av universitets organisasjon, noe som gir et godt grunnlag for å si noe om status og forbedringsmuligheter.

Når det gjelder personvern så vil personvernombudet fremheve følgende forbedringspunkter fra internrevisjonsrapporten:

- Universitetets styringssystem for informasjonssikkerhet og personvern omhandler personopplysningssikkerhet, men dekker ikke personvernområdet i sin helhet. Det er behov for justeringer slik at styringssystemet også definerer styrende krav og føringer for behandling av personopplysninger ved UiT, på linje med informasjonssikkerhet, s. 3.

- Det er ikke etablert tilstrekkelig rapportering på personvernområdet i linjen. Det synes dermed ikke å foreligge en helhetlig oversikt over status på UiTs arbeid innen området tilgjengelig for behandlingsansvarlig s. 5.
- Det er uttrykt behov for større kapasitet på nivå 2, både som et støtteapparat tilgjengelig for de som trenger bistand ved fakultetene/instituttene og også som bindeledd/kontaktpunkt mellom nivå 1 og 2, s. 6.
- Det foreslås at personvern implementeres som et område for eksisterende informasjonssikkerhetsforum, eller at det opprettes et eget forum for personvernområdet, s. 8.
- Etablere metodikk for gjennomføring av personvernkonsekvensvurdering (DPIA), utenom forskningsområdet. Metodikken bør både ta høyde for nødvendig screening av UiTs behandlingsaktiviteter og for selve gjennomføringen av en DPIA i de tilfeller dette er nødvendig, s. 12.
- Gjennomføre screening av UiTs behandlingsaktiviteter og deretter gjennomføre nødvendige DPIA-er basert på en risikovurdering etter at screeningprosessen er ferdigstilt, s. 13.
- UiT har ikke etablert en totaloversikt over alle avtaler som er inngått med leverandører, deriblant databehandlere, s. 14.
- Etablere en bedre dokumentstruktur, med versjonslogg, som gjør det enkelt for brukerne å se hvem som er ansvarlig for dokumentet, når det sist ble oppdatert m.m. Dette vil gjøre det enklere for brukerne å finne korrekt og oppdatert informasjon, s. 17.
- Sikre at studenter er klar over og etterlever kravene som stilles til bruk av UiTs utstyr for studentenes informasjonshåndtering i forbindelse med studentoppgaver, s. 17.
- Utvide den årlige rapporteringen i forbindelse med ledelsens gjennomgang, til også å gi en helhetlig oversikt over status på UiTs arbeid på personvernområdet i linjen, s. 20.
- Sørge for at personvernområdet inntas som en del av opplæringen (nyansatte, ansatte og studenter), s. 22.
- Vurdere hvorvidt hele eller deler av opplæringen på personvern- og informasjonssikkerhetsområdet skal gjøres obligatorisk, s. 22.

Ovenfor er det vist til forbedringsmuligheter. Det er PwCs samlede vurdering at UiT har jobbet godt med personvern og informasjonssikkerhet over tid. Personvernombudet deler denne vurderingen.

Når det gjelder forslaget om forum for personvernombud, så vurderer personvernombudet det som mest hensiktsmessig å utvide mandatet til universitetets informasjonssikkerhetsforum til å omfatte personvern. Forumet møtes ikke så ofte og temaene må være av mer prinsipiell eller overordnet betydning for universitet. Det er også mye overlapp mellom informasjonssikkerhet og personvern og det vil være flere medlemmer som eventuelt måtte være med i begge fora. Men et forum for informasjonssikkerhet og personvern bør suppleres med et internt nettverksgruppe, som møtes regelmessig, ved universitetet og som består av tilsatte som har eller får personvern som en del av sitt ansvarsområde.

5. Personvern i forskning

NSD fører universitetets protokoll over forsknings- og studentprosjekter hvor det behandles personopplysninger. I 2021 ble det meldt inn 762 prosjekter til NSD, mot 649 i 2020. 194 av innmeldingene i 2021 er forskningsprosjekter. De resterende er studentprosjekter, hvorav 468 utgjør mastergradsprosjekter.

I tillegg har universitetet flere store befolkningsundersøker, herunder Tromsøundersøkelsen, hvor det behandles en stor bredde av personopplysninger om tusenvis av personer.

Ved universitetet behandles det med andre ord personopplysninger i stor skala innen forskningsområdet og i stor grad opplysninger som faller inn under særlige kategorier, det som tidligere ble omtalt som sensitive opplysninger.

Omfanget og graden av potensielle konsekvenser for de registrerte i prosjektene og befolkningsundersøkelsene gjør at ivaretakelsen av personvernet er særdeles viktig innen forskningsområdet. Dette stilles store krav til både risikobaserte organisatoriske og tekniske tiltak, herunder at forskere, studenter og forskningsadministrasjonen har tilstrekkelig kompetanse innen personvern.

De fleste henvendelsene til personvernombudet gjelder også behandling av personopplysninger i forsknings- og studentprosjekter.

Innen dette virksomhetsområdet er tjenestene fra NSD sentral. Alle forsknings- og studentprosjekter hvor det skal behandles personopplysninger skal meldes til NSD som vurderer prosjektene i forhold til personvernregelverket etter egen avtale med universitet. Alternativet til å bruke NSD er at universitetets egen forskningsadministrasjon må utføre de samme oppgavene.

Personvernombudets vurdering er at NSD generelt gjør gode vurderinger av prosjektene. De bidrar med spesialistkompetanse innen feltet og robuste tjenester, som det vil være vanskelig og lite hensiktsmessig å bygge opp på egen hånd.

I 2021 har det oppstått spørsmål i sektoren om NSD sin rolle innen forskningsetikk. Rammeavtalen sektoren har med NSD kan forstås slik at NSD har ansvar innen forskningsetikk. Forskningsetikk og personvern henger til dels sammen, men personvernombudet er enig i at det er behov for å vurdere og presisere NSD sitt ansvar og det pågår også et arbeid med å revidere rammeavtalen. Ansvaret for forskningsetikken må alltid ligge til institusjonen og ikke hos NSD. Selv om det har oppstått spørsmål om NSD sitt ansvar, opplever personvernombudet det slik at NSD i praksis viser god rolleforståelse og at de nøyer seg med å be om at eventuelle forskningsetiske spørsmål forankres ved egen institusjon.

En godkjennelse fra NSD er ikke en forskningsetisk godkjennelse. Godkjennelsen er dokumentasjon på at behandling av personopplysninger i prosjektet er vurdert å være i tråd med forpliktelsene etter personvernforordningen. Noen forskere har meldt et behov til personvernombudet om forskningsetisk forhåndsgodkjennelse. Medisinsk og helsefaglig forskning er dekt av REK. Andre forskningsområder har ikke tilsvarende mulighet til å få vurdert forskningsetikken. UiT bør vurdere nærmere behovet for forskningsetisk godkjennelse på andre områder en medisinsk og helsefaglig forskning, og hvordan behovet kan løses.

NSD har rådført seg med personvernombudet om personvernkonsekvensvurderinger (DPIA) i 11 prosjekter i 2021. Dette gjelder DPIA som ble meldt inn i løpet av året. Antallet i 2020 var 13. Forslag til DPIA utarbeides av NSD i samarbeid med prosjektleder. Personvernombudet skal kontrollere gjennomføringen og DPIA godkjennes av institusjonens ledelse. Universitetsdirektøren har opprettet en DPIA-gruppe som vurderer forslagene til DPIA. NSD sin kontaktperson ved UiT, en informasjonssikkerhetsrådgiver, en rådgiver ved Seksjon for forskning og utdanningskvalitet, en rådgiver ved Seksjon for forskning, utdanning og formidling ved Det helsevitenskapelige fakultet og personvernombudet inngår i gruppen.

Etter personvernombudets vurdering har personvernkonsekvensvurderingene innholdsmessig vært i tråd med kravene etter personvernforordningen. Men den totale saksbehandlingstiden har i enkelte tilfeller vært for lang, slik personvernombudet ser det. Dette med den konsekvens at oppstart av behandling av personopplysninger i prosjektet blir forsinket. Samtidig vil personvernombudet understreke at gjennomføring av DPIA ikke er en formalitet og at det ikke er gitt at vurderingen blir godkjent. Ofte blir det satt forutsetninger for godkjennelsen. Universitetet må uansett, i samarbeid med NSD, sørge for at vurderingen av DPIA skjer uten ugrunnet opphold.

All behandling av personopplysninger må ha et lovlig grunnlag i personvernforordningen. Det mest brukte grunnlaget for behandling av personopplysninger i forskningsprosjekter ved UiT er samtykke etter personvernforordningen artikkel 6 nr. 1 a), samt artikkel 9 nr. 2 a) for særskilte kategorier personopplysninger som for eksempel helseopplysninger. Dette gjelder for eksempel universitetets befolkningsundersøkelser og forskningsprosjekter som bruker personopplysninger fra disse undersøkelsene. Det finnes imidlertid et annet grunnlag som personvernombudet vurderer som et bedre og mer robust lovlig grunnlag for behandling av personopplysninger til forskningsformål. Det er personvernforordningen artikkel 6 nr. 1 e) som omfatter behandlinger som er nødvendig for oppgaver i allmennhetens interesse, og for behandling av særskilte kategorier personopplysninger artikkel 9 nr. 2 j) behandlingen er nødvendig for formål knyttet til vitenskapelig forskning. Universitetet bør vurdere å skille tydeligere mellom samtykke til deltakelse i forskning på et forskningsetisk grunnlag og det lovlige grunnlaget for selve behandlingen av personopplysninger, herunder å gå bort fra samtykke som lovlig grunnlag i forskningsprosjekter der det er rettslig grunnlag for det.

6. Personvern i undervisning

UiT har sin strategi for UiT mot 2022 blant annet fastsatt at UiT skal utvikle kunnskap om digital kompetanse i utdanningene. Testing og bruk av teknologi i utdanningen kan innebære behandling av personopplysninger. Før ny teknologi tas i bruk av fagmiljøene er det nødvendig at informasjonssikkerheten og personvernet vurderes og ivaretas. Personvernombudet bør involveres i en tidlig fase.

Et eksempel på et nytt prosjekt innenfor denne strategien, er prosjektet «Student aktiv læring ved testing av e-lærings verktøy i utdanning av operasjonssykepleiere», ved Institutt for helse- og omsorgsfag (IHO). Formålet med prosjektet er å prøve ut og evaluere en ekstern e-læring plattform som kan bidra til mer aktiv og fleksibel læring for studentene for å nå forventede læringsutbytter. E-læringsplattformen gir studentene tilgang til læringsvirksomhet som kan supplere klinisk praksis.

Personvernombudet ble involvert tidlig av IHO ved prosjektleder og de fikk veiledning om hvilke forpliktelser som følger av personvernregelverket. Det ble blant annet inngått databehandleravtale med leverandøren av plattformen og utformet informasjons-/samtykkeskriv for studentene.

UH-sektoren opplever økt antall saker om fusk ved eksamen. Dette i sammenheng med at flere eksamener er gjort om fra skoleeksamen til eksamen som avlegges hjemme. Det er et krav etter lov om universiteter og høyskoler § 3-9 første ledd at kandidatenes kunnskaper og ferdigheter blir prøvet og vurdert på en faglig betryggende måte. Med dette som bakgrunn er det også noen fagmiljøer som ønsker digital overvåkning av kandidatene som avlegger eksamen hjemme. Men overvåkning av studenter i studentenes hjemmemiljø i forbindelse med eksamener reiser flere personvernspørsmål. Unit, nå HK-dir, har startet et arbeid med å kartlegge hvilke retningslinjer eller praksis institusjonene har på området.

Mange studenter behandler personopplysninger ved gjennomføring av intervjuer knyttet til studentprosjekter, både på master- og bachelornivå. Dette gjelder særlig innenfor profesjonsutdanninger, hvor studentene intervjuer yrkesutøvere. Mange studenter har i den forbindelse spørsmål om bruk av privat utstyr til behandlingen av personopplysninger i og med at universitetet i utgangspunktet forbyr bruk av privat utstyr til behandling av personopplysninger. Videre er det slik at det ikke er praktisk mulig å tilby UiT-utstyr til alle studenter som skal behandle personopplysninger i sin utdanning. Personvernombudet er glad for at universitetet høsten 2021 fastsatte nærmere rutiner for unntaksvis bruk av privat utstyr. Dette bidrar til klargjøring for studentene, samtidig som at informasjonssikkerheten blir ivaretatt ved at rutinene følges. Fagenhetene må sette seg inn i disse rutinene med tanke på god lokal veiledning av studentene og deres veiledere om rammene for behandling av personopplysninger i studentprosjekter.

7. Personvern i formidling

På universitetets nettsider finnes det mye informasjon om personvern. I løpet av 2021 har universitetet arbeidet videre med å utvikle uit.no/sikkerhet til å bli en portal for både informasjonssikkerhet og personvern. Dette arbeidet må videreføres med tanke på å få portalen til å dekke hele personvernområdet.

UiTs institusjonelle dataarkiv UiT Open Research Data er et strategisk satsingsområde for universitetet. Det følger av prinsipper og retningslinjer for forvaltning av forskningsdata ved UiT punkt 4.4 at forskeren skal gjøre forskningsdata åpent tilgjengelig for videre bruk for alle relevante brukere, så fremt det ikke er juridiske, etiske, sikkerhetsmessige eller kommersielle grunner til ikke å gjøre det. I denne sammenhengen kan personvernhensyn og personvernlovgivningen være en skranke. Personvernombudet forutsetter at personvernet blir tatt hensyn til i det videre arbeidet med rammene for UiT Open Research Data. UIT bør Utarbeide egen retningslinje og personvernerklæring for tilgjengeliggjøring av personopplysninger i UiT Open Research Data.

UiT bruker Facebook til kommunikasjonsformål. Datatilsynet har i 2021 gjort en grundig vurdering av personvernkonsekvensene ved å skulle opprette en egen side på Facebook. Datatilsynet konkluderte med at de ikke skal benytte Facebook til egen kommunikasjonsvirksomhet. De mener at behandlingen av personopplysninger gjennom å ha en side på Facebook, medfører en for høy risiko for brukernes

rettigheter og friheter. Vurderingen som Datatilsynet har gjort gjelder kun Datatilsynets eget bruk av Facebook og de er tydelige på at dette ikke er en generell vurdering av lovligheten av å bruke Facebook i virksomheters kommunikasjonsarbeid. Men de ønsker en debatt om det offentliges bruk av sosiale medier.

UiT er uansett ansvarlig for at behandlingen av personopplysninger ved bruk av sosiale medier oppfyller kravene etter personvernforordningen. Universitetet må gjøre sine egne vurderinger av sin bruk av sosiale medier. Et verktøy er å gjennomføre risikovurderinger og vurdering av personvernkonsekvenser. Datatilsynets vurdering kan fungere som et utgangspunkt for egne vurderinger.

8. Personvern i administrasjonen

Universitetet behandler opplysninger om studenter og tilsatte til en rekke administrative formål. Personvernombudet vil her peke på noen personvernutfordringer som universitetet må følge opp videre.

I forbindelse med studentutveksling utleveres personopplysninger fra universitetet til verts institusjonen. Utlevering av personopplysninger ut av EØS må ha et lovlig overføringsgrunnlag. Hvis det ikke finnes, er overføringen ulovlig. Vurderingen av de ulike mulige grunnlagene for overføring er komplekse, og det foreligger rettslige uklarheter. HK-dir har i 2021 startet et arbeid må å utrede mulige grunnlag med tanke på klargjøring av rammene for institusjonene. Universitetet må følge opp dette arbeidet og utarbeide egne prosedyrer for vurdering av overføringsgrunnlag for utlevering av personopplysninger i forbindelse med studentutveksling.

Universitetet må ha protokoll over aller behandlingsaktiviteter. For behandlinger til administrative formål fører universitetet egen protokoll. Det pågår et arbeid med å ta i bruk Draftit, som protokollverktøy. Det er nødvendig at universitetet prioriterer dette arbeidet med tanke på å oppfylle plikten etter personvernforordningen og få på plass en funksjonell løsning. Det vil være behov for å gå gjennom innholdet i protokollen, noe alle enheter må ta ansvar for og bidra til.

9. Avvikshåndtering

Personvernombudet skal etter personvernforordningen fungere som Datatilsynets kontaktpunkt ved spørsmål om behandling av personopplysninger ved universitetet.

Datatilsynet har i 2021 ikke tatt kontakt med personvernombudet angående konkrete behandlinger ved universitetet.

Universitetet spør rutinemessig personvernombudet om råd i forbindelse med saksbehandling av avviksmeldinger. I hovedsak har det vært drøftet hvorvidt avviket er av en slik karakter at den må meldes til Datatilsynet.

Personvernombudet erfarer at universitetet følger opp meldinger om brudd på personvernopplysningssikkerheten på en god måte og i tråd med kravene etter personvernforordningen. Personvernombudet oppfatter det også slik at oppfølgningen av avviket skjer i godt samspill med den som melder avviket. Utfordringen er å få meldt inn alle avvikene som måtte skje. Melding om avvik er viktig for å kunne sette i gang tiltak for å forhindre eller redusere konsekvensene for de registrerte og forebygge nye tilfeller.

UiT må brukte NSDs meldingsarkiv aktivt i sin internkontroll av UiTs forsknings- og studentprosjekter meldt til NSD. Av meldingsarkivet fremgår det blant annet en oversikt over prosjekter hvor prosjektansvarlig ikke har svart på sluttmelding fra NSD og oversikt over meldeskjema som ikke er vurdert av NSD på grunn av manglende tilbakemelding fra forsker eller student. I disse prosjektene kan det foreligge avvik i forhold til personvernsikkerheten. UiT må følge opp status for disse prosjektene med forsker eller student og få prosjektstatusen oppdatert i meldingsarkivet. UiT mangler internkontroll rutiner for oppfølgning av meldingsarkivet.

10. Samarbeid og erfaringsutveksling eksternt

UiT Norges arktiske universitet og Samisk høgskole har felles personvernbernombud. Samarbeidet er regulert i egen avtale. Personvernombudet er tilsatt ved UiT som ivaretar personalansvaret for personvernombudet, mens høgskolen betaler for personvernombudstjenesten. Personvernombudet synes ordningen fungerer fint. Personvernombud må ha høye kompetanse innen personvern og jobbe tilnærmet 100 % med personvern for å bygge og opprettholde nødvendig kompetanse. For mindre utdanningsinstitusjoner er det mest hensiktsmessig å dele på et personvernombud.

Det er etablert et nettverk mellom personvernombudene i UH-sektoren. Det er svært nyttig for personvernombudene å kunne drøfte egen rolle og hvordan oppgavene som ligger til rollen kan løses med de andre personvernombudene i sektoren. Det er opprettet en arbeidsgruppe i nettverket, som Personvernombud for UiT og Samisk høgskole leder. På grunn av COVID-19 ble det ikke gjennomført noen fysiske samlinger i nettverket i 2021. Arbeidsgruppen har i stedet gjennomført fire webinarer i nettverket med faglige innlegg fra personvernombudene, samt eksterne innlegg fra SSB, Datatilsynet, NSM og HK-dir.

Det lokale nettverket for personvernombudene ved større virksomheter i Tromsø (UiT, UNN, SpareBank1 Nord-Norge og Tromsø kommune) har ikke gjennomført noen møter i 2021 pga. COVID-19.

11. Risikoområder

Et særskilt risikoområde er overføring av personopplysninger ut av EØS. Risikoen for de registrerte ligger blant annet i at offentlige myndigheter og deres etterretningstjenester kan få tilgang til de registrertes personopplysninger i strid med den registrertes personvernrettigheter i EØS. For UiT ligger risikoen i at personopplysninger overføres ut av EØS uten at det foreligger et rettslig

overføringsgrunnlag etter personvernforordningen eller uten at universitetet har sikret seg at de registrertes personvern er tilsvarende som i EØS. Dette med påfølgende risiko for høyt overtredelsesgebyr fra Datatilsynet og tap av omdømme. Før overføring av personopplysninger ut av EØS må universitet vurdere nøye om det foreligger et lovlig overføringsgrunnlag og vurdere beskyttelsesnivået i mottakerlandet. Dette er en svært kompetansekrevende vurdering og i noen tilfeller må universitetet vurdere hvorvidt landets etterretningslovgivning og landets praktisering av denne går lenger enn det som er nødvendig og proporsjonalt. Dette er rettstilstanden etter Schrems II-dommen i EU. UiT, som behandlingsansvarlig, er ansvarlig for å vurdere grunnlaget for overføring av personopplysninger ut av EØS og UiT må kunne dokumentere sine vurderinger. Videre må universitetet ha oversikt over behandlinger av personopplysninger som innebærer overføring av personopplysninger ut av EØS. UiT bruker flere it-systemer, som innebærer overføring av personopplysninger til USA. Dette ved at leverandøren bruker underleverandører lokalisert der. Direktoratet for høyere utdanning og kompetanse (HK-dir), og Unit, har i 2021 gjennomført en vurdering av de nasjonale systemene som tilbys i sektoren. Disse vurderingene er til hjelp for universitetets egne vurderinger ved bruk av disse systemene. Slik personvernombudet vurderer det ligger risikoen for universitet i større grad ved bruk av andre tjenester enn de nasjonale og ved bruk av tjenester som utelukkende skjer på fakultet eller instituttnivå. Et eksempel på det siste er tjenesten gorilla.sc, som brukes innen forskning. Gorilla.sc har en rekke underleverandører lokalisert i USA, noe som gjør at det er nødvendig å vurdere hvorvidt bruk av tjenesten innebærer overføring av personopplysninger ut av EØS og hva som i så fall er det rettslige grunnlaget for overføringen. Videre er det nødvendig å vurdere overføringsgrunnlag i forskningsprosjekter hvor personopplysninger overføres ut av EØS og ved utlevering av personopplysninger ved studentutveksling.

Avslutningsvis vil personvernombudet peke på det som etter personvernombudets syn generelt innebærer den største risikoen for brudd på forskningsdeltakernes, studenters og de tilsattes personvern og det er utilstrekkelig kompetanse innen personvern hos de som behandler personopplysninger på vegne av universitetet, og da først og fremst kjennskap til grunnleggende personvernprinsipper og interne retningslinjer for behandling av personopplysninger. Alle som behandler personopplysninger ved universitetet må ha tilstrekkelig kompetanse innen personvern, og informasjonssikkerhet, sett i forhold til hvilke rolle og oppgaver de har. Det vil si at universitetet må ha en systematisk tilnærming til internopplæring om personvern innen alle virksomhetsområder ved universitetet. Videre bør universitetet tydeliggjøre hvem som har ansvar for opplæring innen personvern, herunder blant annet å gjøre det klart for fagmiljøene at de selv har ansvaret for å gi veiledning til studenter og deres veiledere om universitetets rammer for informasjonssikkerhet og personvern når studenter skal behandle personopplysninger i sin utdanning. Ideelt sett vil obligatorisk opplæring innen personvern og informasjonssikkerhet for alle vært det beste, men det vil være vanskelig å gjennomføre i praksis med tanke på den store kompleksiteten og variasjonen i de ulike behandlinger av personopplysninger som skjer ved UiT. Men personvernombudet mener at det bør være obligatorisk at personvern og informasjonssikkerhet inngår i all internopplæring. Dette i forhold til ledere, systembrukere, forskere og studentene med deres veiledere. Ansvaret for opplæringen må ligge lokalt hos den enkelte fagenhet eller administrativ enhet med systemeieransvar. Dette fordi universitets egne rammer for informasjonssikkerhet og personvern er sentralt i opplæringen og disse må relateres til målgruppen og de aktuelle behandlingene av personopplysninger.

12. Forslag til tiltak

1. Utvide mandatet til universitetets informasjonssikkerhetsforum til å omfatte personvern og samtidig etablere en gruppe med tilsatte som arbeider med personvern ved ulike enheter, som kan drøfte og ta stilling til personvernspørsmål og hvordan disse bør håndteres i det daglige arbeidet.
2. Vurdere om det er nødvendig å gjennomføre DPIA for enkelte behandlinger, som ikke har forskningsformål. Dersom dette er tilfellet, gjennomføre DPIA for de aktuelle behandlingene.
3. Tydeliggjøre ansvaret for personvernet som ligger til nivå 2 (fakultetene), herunder å synliggjøre/avklare hvem som i det daglige har personvern som del av sitt arbeidsområde.
4. Fastsette internkontroll rutiner for oppfølgning av universitetets meldingsarkiv hos NSD.
5. Vurdere å bruke personvernforordningen artikkel 6 nr. 1 e), samt artikkel 9 nr. 2 j) for særskilte kategorier personopplysninger, i større omfang som lovlig grunnlag for behandling av personopplysninger til forskningsformål.
6. Utarbeide en samlet oversikt over behandlinger og tjenester som innebærer overføring av personopplysninger ut av EØS og fastslå overføringsgrunnlaget for det enkelte tilfellet.
7. Gjøre informasjonssikkerhet og personvern til en obligatorisk del av all internopplæring.