UNIVERSITETET I TROMSØ UiT

RUTINER

for behandling av personopplysninger i forsknings- og student-prosjekter ved Universitetet i Tromsø"

Vedlegg E til "Informasjonssikkerhet ved Universitetet i Tromsø

Fastsatt av: Universitetsdirektøren		Dato: 11.2.2005	
Ansvarlig enhet:	Avdeling for forskning og utviklingsarbeid (AFU)	Kode:	-
Sist endret av: Universitetsdirektøren		Dato: 20.4.2012	
Erstatter:	Versjon av 14.6.2011	Arkivref.:	2010/2582-17
Hjemmel:	Pkt. 1.5 i Instruks for behandling av personopplysninger ved Universitetet i Tromsø		

1. Virkeområde og definisjoner

Disse rutinene gjelder for alle forsknings- og studentprosjekter ved Universitetet i Tromsø som innbefatter behandling av personopplysninger helt eller delvis med elektroniske hjelpemidler.

Definisjoner:
*Personopplysninger***:** Opplysninger som direkte eller indirekte kan identifisere en person. Direkte personidentifiserende opplysninger er navn, personnummer eller andre personlige kjennetegn. Indirekte personidentifiserende opplysninger er bakgrunnsopplysninger som kan gjøre det mulig å spore opplysningene tilbake til en enkeltperson, for eksempel bostedskommune eller institusjonstilknytning kombinert med opplysninger om alder, kjønn, yrke, nasjonalitet, etc.

Behandling av personopplysninger: Enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter.

Behandlingsansvarlig: Universitetsdirektøren, jf. instruksen pkt. 1.

Daglig ansvarlig: Den personen som har det daglige ansvaret for oppfylling av pliktene som den behandlingsansvarlige har, jf. instruksen pkt. 1.

Enhet: Fakultet, TMU eller senter.

Instruksen: Instruks for behandling av personopplysninger ved Universitetet i Tromsø.

Respondent: En som har svart på en undersøkelse/som er undersøkt.

2. Ansvar

Prosjektleder for det enkelte forskningsprosjekt er daglig ansvarlig. Ved tvil avgjør enheten hvem som skal ha det daglige ansvaret. Daglig ansvarlig for studentprosjekter (også ph.d.-prosjekter) er oppnevnt faglig veileder.

Den aktuelle enheten må sørge for etablering av gode rutiner slik at de prosjektene som skal meldes inn blir meldt.

3. Melding til personvernombud
Meldeplikten til Datatilsynet, jf. pkt 9 i instruksen, er erstattet av meldeplikt til personvernombud.

Personvernombud for prosjekter som ikke faller inn under helseforskningsloven
Norsk samfunnsvitenskapelig datatjeneste (NSD) er personvernombud for forsknings- og studentprosjekter som gjennomføres helt eller delvis ved Universitetet i Tromsø og som ikke faller inn under helseforskningsloven.

Planene for behandling av personopplysninger må være godkjent før prosjektet settes i gang. Den daglig ansvarlige skal så snart som mulig, og senest 30 dager før behandlingen av personopplysningene tar til, melde prosjektet. Meldeskjema og veiledning til det finnes på NSDs internettsider: http://www.nsd.uib.no/personvern/

Prosjekter som faller inn under helseforskningsloven
Regionale komiteer for medisinsk og helsefaglig forskningsetikk (REK) er personvernombud for forsknings- og studentprosjekter som faller inn under helseforskningsloven og som gjennomføres helt eller delvis ved Universitetet i Tromsø.

Planene for behandling av personopplysninger må være godkjent før prosjektet settes i gang. Daglig ansvarlig skal melde prosjektet så snart som mulig. Meldeskjema med veiledning og informasjon om behandlingstid finnes på REKs internettsider:
http://helseforskning.etikkom.no/ikbViewer/page/forside?lan=2

4. Informasjon ved innsamling av personopplysninger
Daglig ansvarlig skal sørge for at informasjon blir gitt til respondenten i samsvar med pkt. 3 i instruksen.

5. Innhenting av samtykke
Daglig ansvarlig skal sørge for at samtykke blir innhentet fra respondenten i samsvar med pkt. 4 i instruksen.

6. Behandling av innsynsforespørsler
Alle forespørsler om hva slags behandling av personopplysninger universitetet foretar i forsknings- og studentprosjekter, skal henvises til universitetsdirektøren ved Avdeling for forskning og utviklingsarbeid (AFU). Forespørslene behandles i samsvar med instruksen pkt 5.

Henvendelser om innsyn skal besvares uten ugrunnet opphold og senest innen 30 dager fra den dagen henvendelsen kom inn.

7. Utlevering av personopplysninger
Personopplysninger i forsknings- eller studentprosjektene må ikke utleveres til utenforstående. Utlevering kan likevel skje

1. som informert om ved innhenting av personopplysningene,
2. med samtykke fra respondenten,
3. med hjemmel i lov, eller forskrift gitt med hjemmel i lov.

8. Retting av mangelfulle personopplysninger
Personer som behandler personopplysninger i forsknings- eller studentprosjekter som blir kjent med at det er registrert personopplysninger i prosjektet som er uriktige, ufullstendige eller som det ikke er adgang til å behandle, skal av eget tiltak eller etter krav fra respondenten rette de mangelfulle opplysningene i samsvar med pkt 6 i instruksen.

Dersom den som oppdager slike feil ikke er autorisert til å utføre rettingene, skal feilen meldes til brukere som er autorisert for det.

Henvendelser fra respondenten om retting skal besvares uten ugrunnet opphold og senest innen 30 dager fra den dagen henvendelsen kom inn.

9. Lagring og sletting av personopplysninger
Det skal ikke lagres personopplysninger i forsknings- eller studentprosjekter lenger enn det som er nødvendig for å gjennomføre formålet med behandlingen. Daglig ansvarlig skal sørge for at opplysningene blir slettet.

Personopplysninger kan lagres ved universitetet ut over dette for vitenskapelige formål, dersom samfunnets interesse i at opplysningene lagres klart overstiger de ulempene den kan medføre for den enkelte respondent. Slik beslutning skal treffes av universitetsdirektøren etter forslag fra daglig ansvarlig for behandlingen. Dersom slik lagring besluttes, skal universitetsdirektøren sørge for at opplysningene ikke oppbevares på en måte som gjør det mulig å identifisere respondenten lenger enn nødvendig.

Personopplysninger kan etter søknad fra den daglig ansvarlige lagres hos NSD. Personopplysninger ved alle prosjekter som er støttet av Norges forskningsråd, skal lagres hos NSD.

Daglig ansvarlig skal informere universitetsdirektøren skriftlig når personopplysningene er slettet eller overført til NSD.

10. Risikovurdering
Universitetsdirektøren skal holde oversikt over alle forsknings- og studentprosjekter hvor det behandles personopplysninger.

Enheten skal årlig risikovurdere minst 5 % av sine pågående forsknings- og studentprosjekter. I risikovurderingen skal det klarlegges om sikkerhetskravene i punkt 11 er oppfylt, og sannsynlighet for og konsekvensen av sikkerhetsbrudd skal vurderes.

Risikovurderingen skal foretas av en gruppe nedsatt av administrativ leder av enheten. Minst en forsker og en med IKT-kunnskaper skal være med i gruppen. Universitetet har fastsatt kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger i dokumentet "Informasjonssikkerhet ved Universitetet i Tromsø" punkt 1.1 *Sikkerhetsmål*. Disse kriteriene skal benyttes som et grunnlag for risikovurderingen.

Resultatet av risikovurderingen skal dokumenteres og kopi sendes universitetsdirektøren og den daglig ansvarlige for prosjektet.

11. Sikkerhetskrav
Ved elektronisk behandling av personopplysninger i forsknings- og studentprosjekter, som Universitetet i Tromsø er behandlingsansvarlig for, skal universitetets IT-ressurser benyttes så langt det er mulig.

Direkte personidentifiserbare opplysninger skal ikke lagres elektronisk. Personopplysninger skal avidentifiseres. Direkte personidentifiserbare opplysninger kan unntaksvis lagres elektronisk på universitetets filserver når dette er klart nødvendig ut fra formålet med behandlingen.

Kodeliste, eller annet materiale som kan brukes til å identifisere personene, skal ikke lagres på samme maskin eller filserver.

Hvis private maskiner blir benyttet, skal data lagres i kryptert form slik at ingen andre har tilgang til dataene.

Alle maskiner, deriblant hjemme- og bærbare maskiner, som skal brukes i behandlingen av personopplysningene skal være beskyttet med relevante sikkerhetsmekanismer, herunder blant annet antivirus, brannmur og system for jevnlige oppdateringer.

Den som er daglig ansvarlig er ansvarlig for at det blir tatt jevnlig sikkerhetskopi, backup, av datamaterialet.

Ved bruk av bærbar pc og eksterne lagringsmedier må brukeren være aktsom i forhold til oppbevaring og frakt av utstyret for å minimalisere risikoen for tyveri og skader. Med eksterne lagringsmedier menes minnepinner, CD-/DVD-er, eksterne harddisker, kameraer og lignende.

Dersom opplysningene skal behandles elektronisk ved ekstern virksomhet, skal den som er daglig ansvarlig informere virksomheten om behandlingen og påse at virksomheten oppfyller kravene til informasjonssikkerhet etter personopplysningsloven § 13 og kan dokumentere sitt informasjonssystem og sikkerhetstiltakene.

Privat e-postadresse skal ikke brukes i korrespondanse vedrørende prosjektet.

Universitetet vil etter risikovurdering kunne stille ytterligere sikkerhetskrav til det enkelte prosjekt.

12. Internkontrollrutiner

Avdeling for forskning og utviklingsarbeid (AFU) skal ha ansvaret for revisjon av universitets internkontrollsystem for behandling av personopplysninger i forsknings- og studentprosjekter ved Universitetet i Tromsø, herunder kontrollere ledelsens valg av rutiner og etterlevelsen av rutinene. NSDs system og register over forsknings- og studentprosjekter og REK Nords register skal brukes som et grunnlag i dette arbeidet.

En utpekt tilsatt ved AFU med egen særskilt fullmakt, skal være oppnevnt som kontaktperson overfor NSD og ha ansvaret for å gi informasjon til universitetets forskere og studenter om personvernlovgivningen, melde- og konsesjonsplikt, ordningen med personvernombud, ordningen med arkivering av persondata etter prosjektslutt og universitetets rutiner for behandling av personopplysninger i forsknings- og studentprosjekter.

AFU skal årlig foreta kontroll av et utvalg av pågående forsknings- og studentprosjekter som er meldt til NSD og REK Nord. Formålet med kontrollen er å se om behandlingen av personopplysningene skjer i henhold til universitetets retningslinjer, som opplyst om i melding til NSD, i henhold til eventuelle konsesjonsvilkår og avdelingens eventuelle anbefalte spesielle sikkerhetsrutiner for prosjektet.

Når prosjektet er avsluttet skal AFU kontrollere om personopplysningene har blitt slettet eller overført til lagring, jf. punkt 9.

AFU skal evaluere internkontrollsystemet minst hvert tredje år.