UNIVERSITETET STAVANGER	*Forvaltning av forskningsdata:* Retningslinjer for behandling og oppbevaring av forskningsdata med personopplysninger i studentprosjekter ved Universitetet i Stavanger	
Godkjent av: Personvernombudet på fullmakt	Dato: 27.05.2021	Revisjon nr.: 1.2

Felles retningslinjer for behandling av personopplysninger i studentprosjekter på bachelor- og masternivå ved Universitetet i Stavanger. (Ph.d.-kandidater skal følge retningslinjer som forsker ved UiS).

1. Virkeområde og definisjoner

Disse retningslinjene gjelder for alle studentprosjekter ved UiS som innbefatter behandling av personopplysninger. Kravene til behandling av personopplysninger i studentprosjekter tilsvarer kravene som gjelder for forskere ved UiS. I tillegg gjelder følgende for studentprosjekter:

1. Alle studenter som skal behandle personopplysninger i studentoppgaver plikter å lese informasjon om dette på NSD sine nettsider, og å undersøke om prosjektet må meldes til NSD.
2. Bachelorstudenter anbefales å gjennomføre studentprosjekter uten behandling av personopplysninger, med unntak av **felles innmelding/vurdering**, eller som del av forskerledet prosjekt. Det anbefales å benytte anonyme registerdata eller journaldata, eller andre anonymiserte data. Dersom student og veileder ønsker å gjennomføre studentprosjekter med behandling av personopplysninger, skal NSDs veiledning *Hvordan gjennomføre et prosjekt uten å behandle personopplysninger?* – gjennomgås før endelig beslutning.
3. Studenten skal kun sende inn meldeskjema til NSD i samråd med veileder og dette skal deles med veileder ved innmeldingen hos NSD.
4. Studenten er ansvarlig for å følge opp alle tilbakemeldinger fra NSD, og skal ikke starte opp prosjektet med behandling av personopplysninger før det foreligger tillatelse fra NSD. Studenten bekrefter dette skriftlig til veileder via e-post.
5. Studenten er ansvarlig for å sende beskjed/tilbakemelding til NSD ved prosjektslutt, og bekrefte at alle data er slettet/anonymisert. Studenten bekrefter dette også skriftlig til veileder.
6. Hvis det skal benyttes private enheter i forbindelse med håndtering av innsamlede data (f.eks.: privat PC, båndopptakere mm.) henvises det til punkt om dette i retningslinjene.

Disse retningslinjene er utfyllende til *Politikk for informasjonssikkerhet og personvern ved UiS*, datert 24.09.2019 og *Reglement for informasjonssikkerhet og personvern, datert 02.06.2020.*

Definisjoner:
Personopplysninger: Personopplysninger er all informasjon som kan knyttes til en fysisk person eller personer. Informasjonen kan foreligge som tekst, bilder, video, lydopptak eller elektroniske spor, for eksempel IP-adresser eller aktivitetslogger i IT-systemer. For at informasjonen skal regnes som personopplysninger, må det være mulig å identifisere den eller de personer som opplysningene knytter seg til. (Iht. Personopplysningsloven artikkel 4-1)

Behandling av personopplysninger: Med «Behandling» menes alle operasjoner eller rekker av operasjoner som gjøres med personopplysninger i administrasjon, forskning, kundebehandling ol, enten automatisert eller ikke. Eksempler på dette er innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring. (Personopplysningsloven artikkel 4-2)

Direkte personidentifiserbare opplysninger: En person vil være direkte identifiserbar via navn, fødsels-/personnummer eller andre personentydige kjennetegn.

Behandlingsansvarlig: Rektor er øverste behandlingsansvarlige. Den enkelte enhet er ansvarlig for å iverksette informasjonssikkerhet ved enhetene. Fakultetets ledelse v/dekanen, er ansvarlig for implementering og informasjon til enhetene om disse retningslinjene. Enhetsledere har ansvar for implementering og oppfølging på egen enhet.

Daglig ansvarlig: Den personen som har det daglige ansvaret for oppfylling av pliktene som den behandlingsansvarlige har, for studentprosjekt er det studenten selv og oppnevnt **veileder**. Veileder står ansvarlig for studentprosjekter som meldes til Norsk senter for forskningsdata (NSD). Dersom veileder ikke er ansatt ved UiS når prosjektet avsluttes, må veileder avtale med enhetsleder hvordan ansvaret mot NSD skal følges opp før han/hun slutter som veileder.

2. Ansvar

Studenter og deres veiledere skal sikre at forvaltning av forskningsdata er planlagt og dokumentert i begynnelsen av forskningsprosjektet, og at data med personopplysninger behandles i tråd med disse retningslinjene for innsamling, oppbevaring og lagring. Det gjelder også oppbevaring av dokumentasjonen knyttet til prosjektet, f.eks. NSD-melding, informasjons- og samtykkeskjema.

Det skal vurderes om det er nødvendig å utarbeide en datahåndteringsplan (DMP) for prosjektet, Dersom det er en ekstern finansiør tilknyttet prosjektet må man undersøke om denne stiller krav om bruk av DMP. I så tilfelle, har UiS anbefalt å bruke NSDs mal for Datahåndteringsplan. Planen beskriver hvordan data skal håndteres underveis i prosjektperioden og etter at prosjektet er avsluttet. UiS har utarbeidet egen oversikt over klassifisering og håndtering av ulike typer persondata.

3. Meldeplikt for prosjekter som skal behandle personopplysninger

3.1 Melding til NSD personverntjenester

Norsk senter for forskningsdata (NSD) leverer personverntjenester for UiS. Student- og forskningsprosjekter som behandler personopplysninger, skal meldes til NSD.

Dette gjelder også prosjekter innenfor medisinsk og helsefaglig forskning fra 01.01.2020. Prosjektet skal meldes til NSD senest 30 dager før datainnsamlingen skal starte. For å redusere saksbehandlingstiden hos NSD anbefaler vi at du leser Sjekkliste før innsending av meldeskjema.

Planene for behandling av personopplysninger må være godkjent **før** prosjektet settes i gang.

Hvis det foretas endringer i prosjektopplegget i forhold til de opplysningene som ligger til grunn for NSDs vurderinger, skal endring meldes ved at du logger deg inn på Min side og legger endringene inn i selve meldeskjemaet som angitt på NSDs nettsider..

3.2 Vurdering av forskningsprosjekt i Regional Etisk Komite (REK)
Medisinsk og helsefaglige forskningsprosjekter må søke NSD, og dette kan gjøres parallelt med søknad om etisk forhåndsgodkjennelse hos regionale etiske komiteer (REK).

Alle prosjekter som faller inn under helseforskningsloven skal godkjennes av REK før de settes i gang. REK har en egen portal med opplysninger om frister og behandlingstid. Her er også relevante skjema tilgjengelige. Tilgang til skjema og digital søknad krever brukerkonto.

REK foretar den forskningsetiske vurderingen basert på søknad og forskningsprotokoll med vedlegg. REK kan be om supplerende opplysninger. Prosjektet skal ikke settes i gang før godkjenning fra REK foreligger og veileder som forskningsansvarlig har foretatt en intern vurdering. REK vil sende melding til prosjektleder og forskningsansvarlig om utfallet av REKs vurdering. Daglig ansvarlig skal melde prosjektet så snart som mulig. Meldeskjema med veiledning og informasjon om søknadsfrister og behandlingstid finnes på REKs nettsider.

Daglig ansvarlig for studentprosjekter med personopplysninger er oppnevnt faglig veileder, jamfør NSD meldeskjema.

Lenker til informasjon om meldepliktige prosjekt, meldeskjema, veiledning, informasjons- og samtykkeskjema, samt sentrale begreper finnes på UiS sine nettsider.

4. Informasjon og innhenting av samtykke ved innsamling av personopplysninger

Det er viktig at utvalget/respondentene er godt informert om alle aspekter ved den aktuelle studien, slik at de kan foreta en helhetlig vurdering av hvorvidt de ønsker å delta eller ikke. Det gjelder formål, risiko og mulige gevinster. Det skal derfor utformes et informasjonsskriv der man forespør om deltakelse og informerer om studien.

Samtykket skal være avgitt frivillig, være uttrykkelig og på grunnlag av tilstrekkelig informasjon. Les mer om vilkårene på NSDs nettsider. Her finner du også veiledende mal for informasjon/samtykke.

5. Behandling av forespørsler, retting og sletting

Alle forespørsler om hva slags behandling av personopplysninger universitetet foretar i forsknings- og studentprosjekter, skal henvises til personvernombudet UiS: personvernombud@uis.no

6. Utlevering av personopplysninger/tilgangskontroll

Personopplysninger i forsknings- eller studentprosjektene må ikke utleveres til utenforstående. Det skal være etablert og dokumentert tilgangskontroll til dataene. Normalt vil det kun være student og veileder som har tilgang, i tråd med melding til NSD personverntjenester.

7. 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. Studenten skal bekrefte ved epost til veileder at opplysningene er slettet/anonymisert i samsvar med melding til NSD personverntjenester.

Helseforskningsdata og personidentifiserbare opplysninger skal ikke lagres usikret. Personopplysninger skal avidentifiseres/pseudonymiseres, og lyd-/bildedata skal krypteres (se pkt. 8). Hvis en bruker kodeliste/kodenøkkel, eller annet materiale som kan brukes til å identifisere personene, så skal ikke de lagres på samme maskin eller filserver.

8. Sikkerhetskrav og regler for bruk av privat utstyr.

Når personopplysninger behandles elektronisk på privat datamaskin i prosjekter som Universitetet i Stavanger er behandlingsansvarlig for, skal data lagres i kryptert form slik at ingen andre har tilgang til dataene.

Alle maskiner, også private, som skal brukes i behandlingen av personopplysningene skal være beskyttet med relevante sikkerhetsmekanismer, herunder blant annet antivirusprogram, aktivert brannmur og system for jevnlige oppdateringer av operativsystem og sikkerhetsmekanismer.

Studenten er selv ansvarlig for at det blir tatt sikkerhetskopi, backup, av datamaterialet og at backup blir oppbevart sikret/nedlåst.

Studenten må også være aktsom med tanke på fysisk innsyn på skjermen fra uvedkommende ved valg av arbeidssted når man behandler 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, eksterne harddisker, lydopptakere, kameraer og lignende.

Studenten skal benytte UiS e-postadresse for kommunikasjon/korrespondanse i forskningsprosjektet (privat e-postadresse skal ikke benyttes).

Universitetet v/veileder kan etter vurdering kunne stille ytterligere sikkerhetskrav til det enkelte prosjekt.

8.1 Krav til utstyr/rutiner ved opptak av lyd/ev. video/bilde

Vi viser til UiS sine nettsider når det gjelder regler for bruk av private enheter som mobiltelefon, Ipad eller nettbrett, til innsamling/opptak av lyd eller bilde (se her for mer informasjon om krav til bruk av Zoom, og her for mer informasjon om krav til bruk av Nettskjema). Både video- og lydopptak regnes som personopplysninger.

Studenten har selv ansvar for å skaffe nødvendig utstyr som elektronisk lydopptaker, eller annet påkrevd utstyr som ekstern harddisk, kryptert minnepinne o.l.

Framgangsmåter ved lydopptak/ev. video: UiS har tatt i bruk Nettskjema-appen ved lydopptak. I tillegg må du forholde deg til retningslinjene for Zoom ved bruk av video.

Se mer informasjon om sikkerhetsmekanismer og kryptering på UiS nettsider.

8.2 Viktig å vite om kryptering

Krypteringsmuligheter: Se informasjon om krypteringsmuligheter på UiS nettsider.

Det er **veldig viktig** at man forstår at hvis man krypterer en enhet, eksempelvis en hel harddisk, så vil man tape all informasjon lagret på denne enheten hvis krypteringsnøkkelen og ditt personlige passord mistes. Informasjonen er da tapt og kan ikke gjenopprettes.

> Vær også oppmerksom på at passordbeskyttelse ikke er synonymt med kryptering, eks. data lagret på UiS's hjemmeområder ikke er kryptert.
> Data lagret i sky-tjenester som Google Drive, Microsoft OneDrive, DropBox, etc. er heller ikke kryptert. Legg merke til at selv om mappen/filen du laster opp er kryptert, så er lagringsstedet ikke kryptert. Lagring av personsensitive data (selv om filen er kryptert) i disse tjenestene er dermed juridisk sett ulovlig. Data lagret på personlig/firma-PC, nettbrett, mobiltelefon, kamera-minnekort, ukryptert USB minnepinne etc., er heller ikke sikret i tråd med forskriftene - selv om du har passordbeskyttelse.

9. Melding av avvik

Har det skjedd avvik/feil ved behandling av forskningsdata/personopplysninger?

Avvik skal meldes til:
Student og/eller veileder er ansvarlige for å melde fra om ev. avvik umiddelbart.
Rapportering av brudd eller mulige brudd på personvernet går til Personvernombudet ved personvernombud@uis.no. Veileder bør også informeres dersom student oppdager avvik.

Rapportering av brudd eller mulige brudd på informasjonssikkerhet går til it-hjelp@uis.no