# Retningslinjer for behandling av lydfiler i forskning ved USN

(Retningslinjene er utformet av Avdeling for forskning, innovasjon og internasjonalisering/ Seksjon for forskning og innovasjon)

Lydopptak kan være svært personidentifiserende og dess mer sensitiv informasjon som behandles, dess høyere bør sikkerhetstiltakene være.

## Reduksjon av antall personidentifiserende faktorer i lydopptak

Norsk senter for forskningsdata (NSD) anbefaler i flere prosjekter å instruere de intervjuede til ikke å gi opplysninger som vil øke sannsynligheten for gjenkjennelse. For eksempel opplysninger om geografi som stedsnavn og institusjon intervjuede er knyttet til skal ikke oppgis uten at det er nødvendig for datamaterialet. I noen tilfeller bør du kanskje vurdere pseudonymisering av lyd ved bruk av stemmeskifter/taleforvrengning (egen programvare).

## Opptaksutstyr og bruk av opptaksutstyr

NSD anbefaler ikke å benytte private enheter til datainnsamling, oppbevaring eller lagring, og at bruk av private enheter må avklares med behandlingsansvarlig institusjon (for vår del er det USN). USN har foreløpig ikke en felles utlånsordning for opptaksutstyr, og har derfor utformet disse retningslinjene som det kan vises til hvis det brukes private enheter til lydopptak

I mange tilfeller er forskningsdata så lite personsensitive at de kan lagres på private enheter, så lenge disse behandles forsvarlig. Enheten bør sikres med passord/pinkode, opptaket skal ikke distribueres til uvedkommende og opptaket bør slettes fra enheten så fort det ikke trenger å ligge på enheten lenger, for eksempel når det er overført lagret kryptert (se under).

Du må være bevisst din adferd ved behandling av opptaker, f.eks. ikke legge den fra deg på steder hvor du ikke har kontroll på opptakeren, lås kontoret hvor den oppbevares, ikke lån opptaker ut til uvedkommende osv.

Enheter som har forbindelse med nett bør ikke brukes til opptak av lyd, for eksempel mobiltelefon og nettbrett, hvis det er svært sensitive persondata som skal behandles. Vi anbefaler bruk av diktafon med eksternt minnekort, (eksempelvis Olympus DM-720 og Sony PX4700, ekstra minnekort på 4 GB er tilstrekkelig.)

## Kryptering

Opptaker kan brukes til flere prosjekter samtidig hvis den brukes kun av en person. Men det anbefales at opptak overføres til kryptert enhet (minnepenn, ekstern harddisk) eller at intervju transkriberes så snart som mulig, slik at opptak kan slettes fra diktafon eller mobil.

Se vedlagt orientering om kryptering av data.

Minnebrikker eller disken i lydopptaksutstyr kan til vanlig ikke krypteres.

Dersom en opptaker brukes av flere personer samtidig, skal den kun brukes til ett prosjekt av gangen. Opptakene skal overføres på kryptert enhet og slettes på diktafon så snart som mulig etter opptak. Dersom diktafon skal brukes i nye prosjekt skal nye minnekort benyttes. Gamle minnekort destrueres.

Opptaker skal oppbevares i låsbart skap når den ikke er i bruk, se nedenfor om lagring av lydfiler. Andre krypterte lagringsenheter skal også oppbevares i låsbare skap.

## Redigering og overføring av lydfiler fra en lagringsenhet til en annen

Lydfiler med middels/høy grad av sensitivitet skal ikke redigeres eller lagres på PC tilknyttet nett, dersom de ikke er anonymisert.

Lydfiler kan redigeres på stasjonære og bærbare PCer som ikke har nett-tilkobling, enten permanent eller midlertidig. Med midlertidig menes at trådløst nettilkobling er slått av eller nettkabel er tatt ut. Dersom lydfil er mellomlagret på PC, må du sørge for at den blir fullstendig slettet før nett kobles til.

Med permanent menes at det ikke er teknisk mulig å koble PC'en til nett.

Grad av sensitivitet i materialet avgjør om du bør velge permanent eller midlertidig frakobling fra nett. Sensitivitet øker med omfang av datamengde (antall registrerte, volum av data), men avhenger også av innhold:

- forventning om konfidensialitet kan være stor for opplysninger om helse, velferd, arbeidsforhold.
- Forventning om privatliv (hjem, rekreasjon) kan også være stor
- «Særlige kategorier personopplysninger» har større sensitivitet (helse, rase, religion, fagforeningsmedlemskap, politisk oppfatning, genetiske eller biometriske opplysninger, informasjon om seksuelle forhold eller orientering)
- Husk også at sensitiviteten i «uskyldig» materiale KAN bli stor dersom dette materialet kombineres med andre kilder… derfor bør alle personopplysninger behandles med vekt på konfidensialitet

Du må forsikre deg om at uvedkommende ikke er i det rommet redigering av sensitivt materiale foregår.

## Sletting av lydfiler ved prosjektslutt

Data skal anonymiseres eller slettes etter prosjektslutt, og det innebærer at lydfiler skal slettes.

Data overført til minnekort/minnepinne kan ikke slettes helt sikkert. Etter prosjektslutt skal de destrueres, dersom de ikke skal gjenbrukes av eksakt samme person/personer. Ved gjenbruk av eksakt samme person/personer, bruk programmet CCleaner for å fjerne dataene fra minnekortet/minnepinnen.

Dersom langtidslagring av lydopptak er ønskelig med tanke på oppfølgingsstudier (forskningsformål), skal det søkes godkjenning av NSD og REK.

## Lagring av lydfiler

Lydfiler kan lagres på krypterte minnepenner eller kryptert ekstern harddisk. Ansatte ved USN har kryptert hardisk på ansatt-PC, og ikke-sensitive lydfiler kan som regel også lagres her.

Minnepenner eller eksterne harddisker bør lagres i et avlåst arkiv eller et skap som er adgangsregulert. Står skapet i et rom som er alminnelig tilgjengelig, anbefales det å bruke en safe eller at skapet har to dører, slik at det er vanskelig å bryte opp. Dersom skapet oppbevares i et rom som ikke er alminnelig tilgjengelig, kan det være tilstrekkelig med et ordinært låsbart skap.

Skap må være brannsikret og ha brannvarsler og brannslokkingsapparat/sprinkelanlegg i samme rom, dersom råmaterialet er viktige for å sikre etterprøvbarheten.

Dersom lydopptak lagres på kontoret, skal kontoret låses når du forlater det.

Alternativt kan lydfiler lagres på Tjeneste sensitive data (TSD). Ta kontakt med forskningsdata@usn.no for mer informasjon.

### Arkivering og langtidslagring av lydfiler

Hvis det er ønskelig å bevare dataene for fremtiden, kan lydfiler lagres hos NSD, se NSD sine nettsider om arkivering. Her gis en beskrivelse av hvordan dataene klargjøres for arkivering med blant annet en oversikt over foretrukne filformat og relevant dokumentasjon som skal legges ved, hva som skal fylles ut og signeres og selve forsendelsen.

### Veileder spesielt for helse- og omsorgssektoren

Veileder video-, lyd og bildeopptak i helse- og omsorgssektoren (https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet/normen/veileder-video-lyd-og-bildeopptak-i-helse-og-omsorgssektoren ehelse.no).

# Vedlegg: Kryptering av data

Dette notat er en kort beskrivelse av metode for kryptering av data for å sikre mot innsyn under transport av data og sikring av data lagret på eksterne enheter under feltarbeider.

Informasjon som inneholder personopplysninger eller sensitive personopplysninger skal sikres mot innsyn både under transport av data og når slike data opprettes og lagres utenfor IT-tjenester som normalt behandler slike data. Med transport av data menes forsendelse av data på e-post eller mellomlagring av slike data i skybaserte lagringstjenester. Transport av data kan også være mellomlagring på USB minnepinner for å flytte data fra feltarbeid og til sikker lagring i USN IT-infrastruktur for videre behandling og analyse.

Metodene beskrevet i dette notat erstatter **ikke** lover og regler som gjelder for innsamling og bruk av personopplysninger eller sensitive personopplysninger. Skal det samles inn og forskes på sensitive personopplysninger forutsetter det godkjenning av prosjektet.

Metodene beskrevet i dette notat er for å sikre transport av data som studenter samler inn gjennom feltstudier. De innsamlede data skal overføres til veileder for sikker lagring på USN IT-infrastruktur.

---

Kryptering av filer

Kryptering er metoden som skal benyttes for å sikre data mot innsyn. Det er flere krypteringsmetoder og den som USN skal benytte er en såkalt AES 256 kryptering. AES står for **Advanced Encryption Standard** og **256** er lengden på nøkkel i krypteringsalgoritmen. Lengden på nøkkel har betydning for hvor mye ressurser som må benyttes for å knekke krypertingen.  Denne siden beskriver mer i detalj om AES.

Innhold i en fil som er kryptert med AES åpnes med det samme passord som benyttes for å kryptere dataene.

For å hindre at passordet kommer på avveie skal det sendes i en annen kanal som f.eks muntlig eller via SMS dersom filen sendes på e-post. Passord for å åpne filen skal **ikke** sendes i samme e-post som den krypterte filen sendes.

Det er flere gratis verktøy som støtter kryptering med AES 256. To av de mer stabile verktøy for hhv MS Windows og MacOS er:

- for MS Windows - 7-zip
- for MacOS - Keka

Det er viktig å lese bruksanvisningen for det verktøyet du bruker for å sikre at det er AES 256 som benyttes.

---

## Kryptering av minnepenner

USB minnepenner er usikre medium. Det anbefales derfor at det benyttes to minnepenner for å sikre mot feil på de.

Hvis data som skal transporteres på minnepenner er kryptert før de lagres på minnepennen er det ikke nødvendig med kryptering av selve minnepennen. Minnepennen skal krypteres dersom data som skal lagres på minnepennen er ukryptert.  Kryptering av minnepenner skal gjøres med MS Windows Bitlocker.

Se beskrivelse.

For MacOS kan bitlockerkrypterte minnepenner leses ved å bruke denne tjenesten. Gratisversjonen av appen gir kun mulight for å lese bitlockerkrypterte minnepenner, betalversjonen kan også skrive til bitlockerkrypterte minnepenner.

---

## USN administrerte PC-klienter

Datatrafikken mellom USN administrerte PCer og USNs datasentre er som standard ende-til-ende kryptert. Hardisken på alle USN administrerte PCer blir under installasjon automatisk kryptert. Ansatte i feltarbeid av kortere varighet kan derfor trygt lagre data lokalt på PC. Dette betyr forøvrig ikke at man er sikret mot at hardisken på PCen kan bli defekt. For å sikre seg mot konsekvensen av dette bør man manuelt kopiere data til P: (M:) underveis i feltarbeidet. Alternativt, om en ikke har nettilgang, bør man også her benytte en kryptert minnepinne for backup formål.