Retningslinjer for bruk av Educloud til lagring av sensitive data ved Oslo Nye Høyskole (ONH)

Versjon: 0.1 (utkast)
Gyldig fra: [dato]
Eier: [enhet/rolle, f.eks. Forskningsteknisk ansvarlig]
Godkjent av: [IFL / intern etisk komité / ledelse]

---

1. Formål

Disse retningslinjene skal sikre forsvarlig lagring og behandling av sensitive data (inkl. særlige kategorier personopplysninger) i prosjekter ved ONH, med Educloud som hovedløsning for sikker lagring.

Educloud er utviklet for å kunne lagre **særlige kategorier personopplysninger** i tråd med personvernregelverk, og brukes ved flere institusjoner nettopp for "røde data" og veiledertilgang.

---

2. Omfang

Retningslinjene gjelder for:

- alle forsknings- og studentprosjekter ved ONH som behandler **personopplysninger**, og spesielt **særlige kategorier** (ofte omtalt som "sensitive personopplysninger" eller "røde data"). Retningslinjene gjelder ikke «Svarte data», som skal aldri lagres på Educloud.
- prosjekter hvor Educloud brukes til lagring og/eller etterbehandling av slike data.

---

3. Definisjoner og dataklassifisering

Sensitive data / særlige kategorier personopplysninger omfatter bl.a. opplysninger om helse, politisk oppfatning, religion, genetiske/biometriske data (for entydig identifikasjon) og seksuelle forhold/legning. Datatilsynet peker på at behandling av slike opplysninger i utgangspunktet er forbudt, med unntak der vilkår/grunnlag er oppfylt.

I denne retningslinjen brukes "sensitive data" som en praktisk samlebetegnelse for:

- særlige kategorier personopplysninger (https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/om-behandlingsgrunnlag/spesielt-om-sarlige-kategorier-av-personopplysninger/)
- andre data som ONH klassifiserer som "røde"/særlig beskyttelsesverdige

---

4. Roller og ansvar

Prosjektleder

- Har det overordnede ansvaret for at prosjektet følger disse retningslinjene.

- Skal sikre at databehandlingsplan, tilgangsstyring, lagring, overføring og sletting er dokumentert og etterlevd.

Forskningsteknisk ansvarlig (FTA)

- Gir rådgivning om sikker databehandling, mappe-/tilgangsoppsett i Educloud, og etterlevelse av disse retningslinjene.
- Har ansvar for sikkerhetsmessig oppsyn med særskilte risikopunkter (se punkt 10).

Intern etisk komité / IFL

- Vurderer prosjektets etiske og organisatoriske forutsetninger, og skal sammen med FTA gjennomgå prosjektsøknad og databehandlingsplan ved behandling av sensitive data.

Intern ONH-ansatt tilknyttet prosjektet ("intern ansvarlig")

- En intern ONH-ansatt skal være tilknyttet alle prosjekter som lagrer sensitive data i ONHs Educloud.
- Den interne ansvarlige:
    - skal alltid ha tilgang til data så lenge de eksisterer
    - skal ha oversikt over hvor data ligger
    - skal påse at data lagres forsvarlig og slettes ved prosjektslutt
    - skal være involvert før studenter lagrer eller flytter data i Educloud

Studenter

- Skal ikke lagre sensitive data i Educloud uten i samråd med intern ansvarlig.

---

5. Obligatoriske krav før datainnsamling starter

Før innsamling/behandling av sensitive data kan starte skal følgende være oppfylt:

1. **Meldeskjema til Sikt**
   Alle prosjekter som behandler personopplysninger i forskning/studentprosjekt skal sende inn Sikts meldeskjema når institusjonen har avtale med Sikt. Man må vente på vurdering før prosjektet kan starte.
2. **Søknad til intern etisk komité ved ONH**
   Alle prosjekter som skal behandle sensitive data må søke intern etisk komité om godkjenning (evt. andre godkjenninger dersom prosjektet krever dette).
3. **Gjennomgang av databehandlingsplan**
   For prosjekter med sensitive opplysninger skal FTA, sammen med IFL/intern etisk komité, gjennomgå prosjektsøknad og databehandlingsplan for å sikre:
    - forsvarlig lagringsløsning
    - tilgangsstyring (minste privilegium)
    - sikker overføring

- plan for sletting/retensjon
- håndtering av fysiske dokumenter og nøkler

---

6. Lagring i Educloud (hovedregel)

1. **Plassering**
   - Alle prosjekter som behandler sensitive data skal lagre disse i **sikker mappe** på ONHs Educloud-prosjekt, med mindre noe annet er eksplisitt avtalt.
2. **Tilgangsstyring**
   - Kun personer med tjenstlig behov skal ha tilgang.
   - Intern ansvarlig (ONH-ansatt) skal alltid ha tilgang så lenge data eksisterer.
3. **Forbud mot lagring utenfor sikre områder**
   - Sensitive data skal ikke lagres i åpne, uavklarte eller felles områder i Educloud.

---

7. Datainnsamling via Nettskjema – særskilt ONH-policy

Nettskjema kan i noen institusjonsoppsett kobles direkte til Educloud for sikker lagring. Ved ONH er dette **kun tillatt når tilganger er konfigurert korrekt før datainnsamling starter**, og når intern ansvarlig (ONH-ansatt) er involvert.

- Direkte kobling Nettskjema → Educloud (tillatt kun ved sikker konfigurasjon)
  Direkte kobling kan benyttes dersom alle følgende krav er oppfylt:
  - Tilganger er strammet inn før innsamling: eventuelle standard-/gruppe-tilganger (f.eks. *ec<prosjekt>-member-group*) skal fjernes, og kun navngitte personer skal ha tilgang. Minimum: skjemaeier + admin-/støttegruppe + evt. veileder/intern ansvarlig.
  - Skjemaeier skal ha nødvendige rettigheter (lese/endre/slette) for å kunne administrere data.
- Dersom sikker tilgangskonfigurasjon ikke er mulig (teknisk eller organisatorisk), er direkte kobling ikke godkjent. Da skal prosjektet benytte manuell overføring fra Nettskjema til riktig sikker mappe i Educloud, og overføringen skal dokumenteres (dato, ansvarlig, hva som er flyttet og hvor det er lagret).
- Før datainnsamling starter skal intern ansvarlig bekrefte (skriftlig i prosjektets dokumentasjon) at tilgangsoppsettet er kontrollert og i tråd med punkt 7.1.

---

8. Flytting/utlevering av sensitive data ut av Educloud

- Det er **ikke lov å flytte sensitive opplysninger ut av Educloud** med mindre dette er **eksplisitt avtalt og dokumentert** (f.eks. i databehandlingsplan/vedtak).

- Ved godkjent unntak skal det fremgå:
    - hvorfor flytting er nødvendig
    - hvilken løsning som brukes
    - hvordan tilgang, kryptering, logging og sletting håndteres
    - hvem som er ansvarlig

---

9. Fysiske sensitive opplysninger og nøkkelmateriale

- ONH skal ha en **låsbar safe** for oppbevaring av:
    - fysiske dokumenter med sensitive opplysninger (f.eks. samtykkeskjema på papir)
    - kodenøkler, koblingslister og annet fysisk nøkkelmateriale tilhørende prosjekter
- Det skal være tydelig definert:
    - hvem som har tilgang til safen
    - hvordan tilgang tildeles og trekkes tilbake
    - hvordan utlån/innlevering loggføres (minstekrav: dato, navn, formål)

---

10. Sikkerhetsprosedyrer: oppsyn, forebygging og opprydding

1. **Forebygging av feilplassering i Educloud**
    - Educloud skal rigges slik at ingen kan legge filer i "åpne" deler av mappesystemet uten tydelig eierskap/tilgangskontroll.
    - Hvis dette ikke lar seg løse via tilgangsstyring, skal det innføres en operativ prosedyre, f.eks.:
        - **daglig opprydding/sletting** av data som er lagt i åpne/ukontrollerte områder
        - tydelig intern kommunikasjon om at slike områder ikke skal brukes
2. **Oppsyn med nettskjema.educloud.no**

FTA skal føre regelmessig oppsyn med nettskjema.educloud.no for å avdekke skjemaer som har uønsket bred tilgang (f.eks. *ec95-member-group* eller tilsvarende).

Dersom et slikt skjema oppdages, skal FTA iverksette følgende tiltak i prioritert rekkefølge:

1. **Identifiser og varsle eier:** Forsøk å identifisere skjemaeier/prosjektleder og varsle intern ansvarlig og relevant enhet.
2. **Sikre data på riktig sted:** Dersom skjemaet inneholder (eller kan inneholde) sensitive data, skal data **flyttes til prosjektets sikre mappe** i Educloud (evt. eksporteres og lagres i sikker mappe) i samråd med intern ansvarlig.
3. **Tidsfrist og videre håndtering:** Dersom eier ikke kan identifiseres eller ikke responderer innen en kort frist (f.eks. 5 virkedager), skal skjemaet slettes.

---

11. Sletting, prosjektavslutning og etterlevelse

- Ved prosjektslutt skal sensitive data slettes fra Educloud i tråd med:
    - prosjektets databehandlingsplan
    - eventuelle vedtak/godkjenninger
- Intern ansvarlig (ONH-ansatt) har ansvar for å:
    - påse at sletting faktisk gjennomføres
    - dokumentere at sletting er utført ved å melde avslutning/anonymisering til Sikt.

---

12. Avvik og sikkerhetshendelser

Eksempler på avvik:

- sensitive data lagret utenfor sikker mappe
- direkte Nettskjema→Educloud-kobling brukt
- data flyttet ut av Educloud uten eksplisitt avtale
- mistet fysisk materiale/nøkkelmateriale

Ved avvik skal man:

1. stoppe videre behandling/deling der det er mulig
2. varsle FTA og intern ansvarlig umiddelbart
3. sikre spor/dokumentasjon (hva skjedde, når, hvem, hvilke data)
4. gjennomføre opprydding og forebyggende tiltak

---

13. Revisjon og vedlikehold

- Retningslinjene bør revideres minimum årlig, og ellers ved:
    - endringer i Educloud-oppsett
    - endringer i prosesser for Nettskjema
    - avvik som viser behov for tydeligere krav
